HACKER JOURNAL

N° 214

SECURITY

TOKEN RSA COMPROMESSI A RISCHIO MILIARDI DI TRANSAZIONI ONLINE

ANDROID CONTRO TUTTI

Installa e usa tutto il software che vuoi!

PROGRAMMING

UNA APP PER AGGREGARE DATI DAI SOCIAL NETWORK

HACKER JOURNAL N° 214 - MENS - ANNO 12 - € 2,00

STAY HUMAN

Viviamo circondati da una nuvola di elettronica: cellulari, televisori, bancomat, orologi di precisione atomica e migliaia di altre diavolerie che accumuliamo e che ci rendono la vita più facile e che, in alcuni versi, parlano di noi al mondo intero.

Di questa nuvola fa naturalmente parte anche la nostra vita virtuale, i nostri avatar, proiettati sul Web nei nostri account Facebook, nei nostri blog, nelle foto condivise con Flickr e in mille interventi nei forum. Proiezioni che spesso sono accusate di dire troppo di noi, di raccontarci più di quanto vorremmo fare, che si lasciano consultare e smontare da motori di ricerca e società di marketing, 24 ore su 24, 365 giorni all'anno. Proiezioni che continuano a rappresentarci anche quando non ci siamo perché dormiamo, perché siamo in vacanza oppure perché il nostro fisico arriva alla fine del suo cammino. Anche quando si arriva a questi estremi, i nostri ego di bit continuano a rappresentarci, dando modo a chiunque di conoscere se non la sostanza, l'ombra di chi li ha creati, voluti e coltivati.

C'era un uomo che si chiamava Vittorio Arrigoni ma questo era solo il suo real name. Quelli che seguivano il suo blog, guerrillaradio.iobloggo.com, lo conoscevano come Vik. Un alias senz'altro più comodo per chi, come lui, cercava di portare la pace tra popolazioni dove il suo nome vero risultava di difficile pronuncia.
Un nick amichevole per un blog dove vigeva, come dice il primo post, del 23 luglio 2004, giorno della Rivoluzione di Libia ed Egitto, "il diritto di inveire, denunciare, soverchiare, sconvolgere". Dopo questo annuncio, una valanga di post sulla guerra, sulla pace, sull'umanità, sulla sua vita da volontario di pace. L'ultimo post è del 13 aprile di quest'anno. Non ce ne saranno altri.
Vik è stato ucciso nella striscia di Gaza il giorno dopo.

A noi resta un'eredità di preziosi bit che ci raccontano di lui e ci ricordano, come lui ribadiva in calce ad ogni singolo post, che dobbiamo restare umani.

Sommario

laboratorio@hackerjournal.it Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".
posta@hackerjournal.it È l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.
redazione@hackerjournal.it Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

ANNO 12 - N. 214
GIUGNO 2011

Mensile - 2,00 euro
www.hackerjournal.it

Sprea International
Via Torino, 51
Cernusco Sul Naviglio (MI) - Italy
Tel. (+39) 02.92.43.21
Fax (+39) 02.92.43.2.236

Direttore responsabile:
Luca Sprea - direttore@hackerjournal.it

Redazione:
redazione@hackerjournal.it

Stampa: Arti Grafiche Boccia S.p.a. - Salerno
Carta: Valpaco Paper Supply Chain Optimizer

Distribuzione:
M-Dis Distribuzione Spa
Via Cazzaniga, 19 – 20132 Milano

HACKER JOURNAL
Pubblicazione registrata al Tribunale di Milano il 27/10/03 con il numero 601

VINCE SONY?

di M45t3r EWS
redazione@hackerjournal.it

FINISCE CON UNA VITTORIA PER SONY LA SFIDA CONTRO GEOHOT PER L'HACK DELLA PS3.

Una vicenda che sembra tratta da un film e gli ingredienti ci sono tutti: una tecnologia segreta, una major dalla voce grossa, il geniale ragazzino che trova una falla. Un film che sembra già visto ma con un finale a sorpresa e fin troppo realistico: la major tira fuori il portafogli e stringe un accordo di ferro col ragazzo, vincolandolo al segreto perpetuo e stipulando un vero e proprio contratto per il futuro, fatto di penali nel caso in cui questo si lasci prendere la mano e divulghi informazioni.
Tutto iniziò alla fine di gennaio del 2010 con la pubblicazione da parte di George Hotz (geohotgotsued.blogspot.com) di un post in cui annunciava di essere riuscito a leggere e scrivere dalla blindata memoria della sua PS3. Hotz non è propriamente il primo che passa per strada: nel 2007 si è inventato Imaging 3D (chiamato anche Progetto Ponte Ologrammi) che gli è valso la sponsorizzazione di qualche migliaio di dollari targati Intel. Così, Sony non ha certo ignorato l'annuncio, anche perché questo è stato seguito da diversi exploit. Cose inutilizzabili, sicuramente, ma che davano certamente preziose indicazioni a Sony che non si aveva a che fare con casi fortunati: GeoHot stava veramente facendo a pezzi la PS3. Dall'altra parte, Sony ha replicato con aggiornamenti continui del sistema. Grazie a questo lavoro è stato permesso l'uso di dongle USB e l'installazione di firmware custom. L'inizio vero della battaglia è datato 12 gennaio 2011, giorno in cui Sony ha dato il via a una causa legale contro GeoHot per violazione dei diritti d'autore. Il 27 gennaio, il tribunale del distretto del Nord della California ha vietato esplicitamente a GeoHot qualsiasi rilascio di informazioni sul jailbreak della PS3. GeoHot ha replicato con scherno, pubblicando un video contro Sony in cui ha nascosto le chiavi del firmware 3.56 e peggiorando ulteriormente la sua situazione. Nel frattempo è partita la campagna di solidarietà che ha iniziato a raccogliere soldi per contribuire alle spese processuali. L'hacker ha annunciato sul suo sito campagne di boicottaggio contro Sony, proclami contro il colosso e così via. Alla fine, tutto è sembrato svanire nel nulla e nessuno più parlava di GeoHot: sul suo blog sono terminati gli annunci contro Sony e tutto è diventato più fumoso.
Fino a circa la metà di aprile, quando trapela il motivo di questo silenzio: Sony ha aperto il portafogli ed ha fornito a GeoHot un sostanzioso contributo per stare zitto e non rivelare più nulla.
Il finale inaspettato di una vicenda che poteva essere epica e ha infiammato diversi attivisti: GeoHot, novello Davide contro Golia. Invece Davide è passato dalla banca a ritirare i soldi, Golia ha vinto e l'accordo, alla fine, è anche amichevole: in futuro, GeoHot potrà essere costretto a pagare fino a 250.000 dollari nel caso in cui riveli qualcosa della tecnologia Sony.
Fine? No: questo accordo viene visto come un tradimento di GeoHot verso la comunità hacker e i commentatori sul suo forum si sono scatenati pro e (soprattutto) contro.
In particolare, Night Breed ha chiesto a GeoHot di rendere conto dei soldi raccolti per la tutela legale e a guadagnarci è stata la EFF. Per liberarsi degli (presumiamo) inutili spiccioli raccolti, GeoHot ha donato 10.000 dollari alla Electronic Frontiers Foundation. Adesso, però, si è aperta la caccia perché Sony non sembra essere riuscita a rimediare alle falle scoperte da GeoHot. Lo ha solo fatto tacere. Ora, quindi, il lavoro tocca a noi. Nel peggiore dei casi, Sony pagherà ancora. Sarà ammesso l'uso personale delle falle trovate?

Hello George Hotz,

You authorized a payment of $10,000.00 USD to Electronic Frontier Foundation (accounting@eff.org)
Your funds will be transferred when the merchant processes your payment. Any money in your PayPal account at that time will be used before any other payment source.

Thanks for using PayPal. To see the full transaction details, log in to your PayPal account.

It may take a few moments for this transaction to appear in your account.

Merchant
Electronic Frontier Foundation
accounting@eff.org
415-436-9333

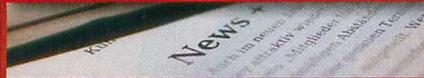
Instructions to merchant
You haven't entered any instructions.

Description	Unit price	Qty	Amount
	$10,000.00 USD	1	$10,000.00 USD

Subtotal $10,000.00 USD
Total $10,000.00 USD

Payment $10,000.00 USD

Payment sent to accounting@eff.org

La ricevuta del trasferimento via Paypal a EFF. 10.000 dollari... 30 denari e l'inflazione di 2000 anni per tradire i propri ideali?

VISITE (SGRADITE) A WP

di M45t3r EWS
redazione@hackerjournal.it

MIGLIAIA DI ACCOUNT WORDPRESS A RISCHIO.

Non c'è pace per Wordpress: dopo la serie di attacchi DDOS di marzo che hanno portato a un servizio a singhiozzo, ora è la sicurezza dell'intero ecosistema WP a rischiare. Alcuni criminali, infatti, hanno bypassato i sistemi di sicurezza arrivando a prendere possesso di diversi server e a sottrarre sia il codice sorgente (problema di poco conto visto che è Open Source), sia dati appartenenti ad Automattic e ai suoi partner, creatori della nota piattaforma. Queste informazioni, di cui Matt Mullenweg, presidente della società, non ha precisato la natura, sembrano includere anche le password di accesso ai blog degli utenti e diverse informazioni sensibili. La stessa Automattic ha informato gli utenti del serio problema, chiedendogli di modificare quanto prima le loro credenziali di accesso, anche nei siti esterni all'ecosistema WP e in cui la password trafugata è stata, eventualmente, riutilizzata.
Ovviamente mister Mullenweg afferma che stanno lavorando per migliorare la sicurezza, che le autorità stanno indagando e così via ma la domanda è lecita: come mai una società di importanza mondiale, leader nel suo campo e detentrice di un prodotto così conosciuto non ha pensato prima al problema? Che senso ha che si concentrino solo ora su un punto che, per una piattaforma che occupa spesso idee scomode, risulta così cruciale? Sembra una storia già vista, che ricorda un detto popolare: inutile chiudere il recinto quando i buoi sono ormai scappati.

ARRIVA NATTY NARWHAL

di N4break
redazione@hackerjournal.it

PRONTO UBUNTU 11.04 CON INTERFACCIA UNITY E LIBRE OFFICE.

Nel momento in cui scriviamo, Canonical ha annunciato che l'ultima release di Ubuntu Natty Narwhal sarà anticipata da una beta, diversamente dall'abitudine che vede le release anticipate da almeno una versione RC. Questa decisione è stata presa per aumentare il tempo disponibile per i test necessari da parte della community, anche considerando le sostanziali novità che vengono introdotte dalla versione 11.04. Quella più attesa è senz'altro l'integrazione dell'interfaccia Unity in sostituzione di Gnome, una scelta che ha portato a qualche polemica ma che trova il suo fondamento nella diminuzione della complessità dell'interfaccia Gnome. Unity raggruppa i menu Gnome in una sidebar laterale integrata, come fa la taskbar di Windows 7.
I lati negativi, purtroppo, non mancano visto che questa barra non sarà personalizzabile: niente widget o extra. Non si potrà, per ora, nemmeno spostare in altre parti dello schermo. Una scelta fatta per venire incontro a necessità di semplificare l'ambiente, richieste dagli utenti meno esperti. Poco male, però, per chi non desidera avere a che fare con questi limiti: direttamente al login si potrà scegliere di usare la tradizionale shell Gnome. Altra grande novità la presenza di Libre Office, una specie di secondo debutto dopo la bufera Oracle su OpenOffice.org e la rinuncia a una versione commerciale della suite. Per finire, la NetBook Edition integra la versione Desktop: un sintomo dell'ottimizzazione del codice e delle distribuzioni disponibili e ulteriore passo verso la semplificazione per gli (inesperti) utenti comuni.

BACKBOX LINUX

di Andrea Draghetti
redazione@hackerjournal.it

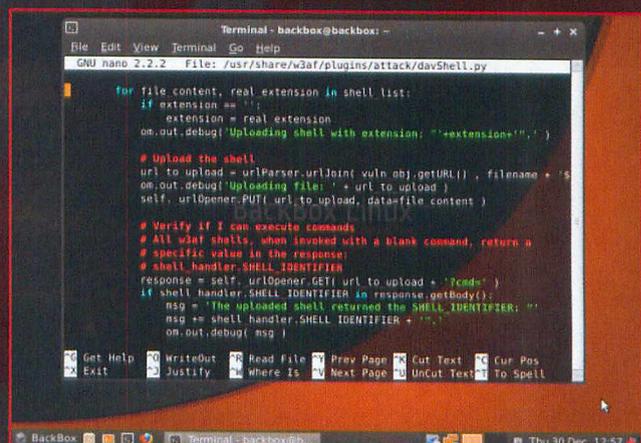
Flexible Penetration Testing Distribution

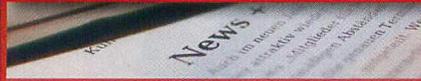
BackBox Linux
FLEXIBLE PENETRATION TESTING DISTRIBUTION

BackBox Linux è un sistema operativo basato su Ubuntu distribuito come Live CD e orientato al penetration testing.
Il progetto tutto italiano vede la luce nel Maggio 2010 con il rilascio della prima beta, nonostante sia una distribuzione giovane già nella sua prima uscita ha suscitato un enorme interesse. Il team di sviluppo è costantemente al lavoro e gode del supporto di una fiorente comunità.
BackBox è basata sull'ambiente desktop Xfce o FluxBox, è progettata per fornire un'interfaccia semplice, intuitiva e allo stesso tempo completa e potente. Il tema di default mescola l'eleganza di un tema scuro con l'usabilità di un tema luminoso. I punti di forza di questa distribuzione sono l'estrema semplicità di utilizzo, l'ottimo riconoscimento e supporto dell'hardware, le ottime prestazioni anche su computer meno recenti ed il vasto parco software rivolto al penetration testing.
La scelta dei vari tools risulta particolarmente accurata: sono suddivisi per categoria ed inoltre sono installati solo i programmi essenziali per effettuare i test di sicurezza, ma se si vuole estendere il pacchetto software si può tranquillamente ricorrere ai suoi repository PPA.

Eccovi un breve riepilogo suddiviso per categoria:

- Wireless Analysis (Aircrackg-ng, kismet, ecc.)
- Web Application Analysis (cms-explorer, sqlmap, ecc.)
- Privilege Escalation (wireshark, medusa, ecc.)
- Vulnerability Assessment (msf, ecc.)
- Network Napping (zenmap, nbtscan, ecc.)
- Maintaining Access (weevely, ecc.)

BackBox è disponibile sia in versione 32bit che 64bit, entrambe avviabili in modalità Live. Ovviamente si consiglia di installare il sistema operativo su hard disk per godere a pieno delle sue funzionalità. A differenza di altre distribuzioni orientate al penetration testing, BackBox è ottima anche per un utilizzo desktop.
È possibile scaricare le ISO dal sito ufficiale www.backbox.org, dove potrete anche trovare la documentazione e i video tutorial messi a disposizione dalla community e aggiungerne anche di vostri.
BackBox è una distribuzione hacker friendly, chiunque può partecipare allo sviluppo del progetto ed è il benvenuto. Non vi resta dunque che iscrivervi sul forum e partecipare alle discussioni oppure accedere al canale IRC ufficiale #BackBox sul server Autistici.

Ricca la dotazione di software disponibile in questa distro, non limitata solo ai programmi dedicati all'hacking.

Ovviamente, tra i tool non può mancare un terminale. Backbox è adatto all'uso in contesti molto variegati.

20 ANNI DI LINUX

di N4Break
redazione@hackerjournal.it

LINUX VS WINDOWS: DICONO CHE IL PINGUINO ABBIA VINTO.

Jim Zemlin, direttore esecutivo di Linux Foundation, ha ultimamente rilasciato una dichiarazione piuttosto forte: " Semplicemente, Microsoft non ci interessa più di tanto. Era il nostro più grande rivale ma ora è come prendersela con un cucciolo". Motivazione dell'esternazione, che ha fatto sorridere Microsoft, la celebrazione del ventesimo compleanno di Linux, occasione in cui Zemlin ha ulteriormente rincarato la dose affermando che Linux ha oramai conquistato quasi tutti i mercati che c'erano da conquistare: dall'IT all'elettronica di consumo. Unica ammissione di parziale sconfitta è quella del mercato dei PC, desktop e laptop dove, comunque, Zemlin ha annunciato novità e più incisività.
Ci permetta mister Zemlin ma, probabilmente, dall'alto della sua carica alla Linux Foundation pensiamo abbia preso una cantonata di portata epocale. Noi, qui in trincea, possiamo assicurarle che la stragrande maggioranza degli utenti non sa cosa sia Linux, non ha idea che esistono distro differenti con caratteristiche differenti, confonde persino Linux e OsX.
La maggior parte degli utenti non ha nemmeno idea di essere circondati da dispositivi con Linux embedded e, alla fine, non gli importa: basta che sul loro desktop possano mettere i loro giochi, che le loro abitudini cambino il meno possibile.
Quanto ai server, l'argomento è quanto meno spinoso, visto che la tendenza attuale è quella di avere una macchina Linux che virtualizza VM Windows oppure tante macchine Linux dedicate ognuna ad un servizio ben definito. Una condizione che difficilmente viene replicata con Windows, che solitamente funziona in condizioni ben differenti. Senza contare alcuni dettagli come oltre l'80% del mercato dei Directory Services detenuto da Active Directory, oltre il 50% delle installazioni di database detenuto da SQL Server, l'uso di Windows nell'80% delle installazioni SAP. Il tutto complicato dall'acquisizione di Sun da parte di Oracle, che ha un Solaris da mettere sul tavolo insieme al suo Db.
Ci scusi mister Zemlin ma, dalla prima linea, le cose sembra che funzionino ma non che siano così esaltanti.

HACKER? IN GALERA!

di Little Rose
redazione@hackerjournal.it

LA VOGLIA DI PROTAGONISMO TRADISCE IL CRACKER DI TURNO CHE VINCE UN SOGGIORNO NELLE GALERE FRANCESI.

In TV, oggi, passa proprio di tutto: da finte casalinghe quasi disperate a gente che fa del litigio sulle stupidaggini una scienza che esercita continuamente. Capita anche, alla TV francese, di vedere un tizio che si proclama hacker, che dice di aver violato le reti dell'esercito d'oltralpe, che dice di essere penetrato nei sistemi di sicurezza della Thales Security e cose così. Ovviamente tutto finto perché nessun Cracker dovrebbe mai proclamarsi Hacker. Così come nessun Cracker si proclamerebbe mai tale. Tanto meno in TV. Vantarsi poi di essere entrati in una rete, per di più dell'esercito, invece, è da premio Ignobel. Il tutto coinvolgendo, poi, l'organizzazione Anonymous, che non ha certo come scopo il Cracking!
Onestamente pensavo, come tutti, che si trattasse di un millantatore, come ce ne sono tanti in TV, anche nelle TV estere. Invece no: non era un millantatore. Era veramente uno stupido. Dopo qualche giorno di indagine, la gendarmeria francese lo ha arrestato con accuse pesantissime: accesso non autorizzato a sistemi informativi riservati, furto di dati e truffa. Un costo tutt'altro che trascurabile in cambio di qualche minuto di notorietà. A completare il quadro desolante, la beffa: l'unica cosa su cui sembra aver mentito è stata la sua adesione ad Anonymous. L'unica parte della sua confessione pubblica che non sarebbe stata perseguibile per legge.
Semmai ci capitasse di andare in TV, ricordiamoci che non siamo al bar con gli amici e che un vero hacker lo è prima di tutto nello spirito. Non lo è per farsi bello. Quelli sono i lamer: gente che solitamente non viene amata in modo particolare.

APRIAMO GLI AIR PORT

di N4Break
redazione@hackerjournal.it

Sbloccato, finalmente, l'AirPlay. Streaming libero per tutti!

Come molti colleghi, trovo che l'AirPlay sia affascinante: si prende una vecchia, la si rinnova a sufficienza per metterci un po' di protezioni e la si rimette sul mercato con un nome accattivante, qualche lucchetto e via! Pronti per spennare il pollo di turno. È stata con una risata, quindi, che gli addetti hanno accolto la notizia che James Laird, sviluppatore indipendente, ha trovato la chiave privata usata per la codifica dello streaming dall'Airport Express.
Il concetto di questo aggeggio è banale: accoglie musica in streaming, la codifica, la lucchetta e la rimanda wireless a dispositivi compatibili prodotti su licenza Apple. Poco importa che lo streaming in ingresso non sia protetto: il meccanismo non serve per evitare che qualcuno rubi la nostra musica ma è palesemente utile ad Apple che vende le licenze necessarie per i ricevitori. Da questo punto di vista, la scoperta della chiave privata da parte di Laird e la sua decisione di avviare un progetto Open Source che possa rendere libero AirPlay è, per Apple, una batosta colossale. Tutto è nato dalla volontà di Laird di aiutare la sua ragazza a risolvere i problemi che aveva con il suo Airport Express. Così è praticamente stato costretto a fare un dump della ROM e a lavorare di reverse engineering. Cosa non può fare l'amore? Da questa esperienza, Laird ha dato vita a un progetto, https://github.com/albertz/shairport, che integra un server RAOP e che potrebbe arrivare a supportare flussi multipli di stream. Di certo, Apple non starà a guardare e promette guerra a Laird e a tutte le aziende che cercheranno di usare la chiave per produrre hardware compatibile senza licenza. Scommettiamo già, però, che software come VLC (a cui Laird ha inviato immediatamente la chiave) non si faranno problemi per ricevere in streaming i contenuti di iTunes.

GOOGLE VOLA E (NON) CADE

di Little Rose
redazione@hackerjournal.it

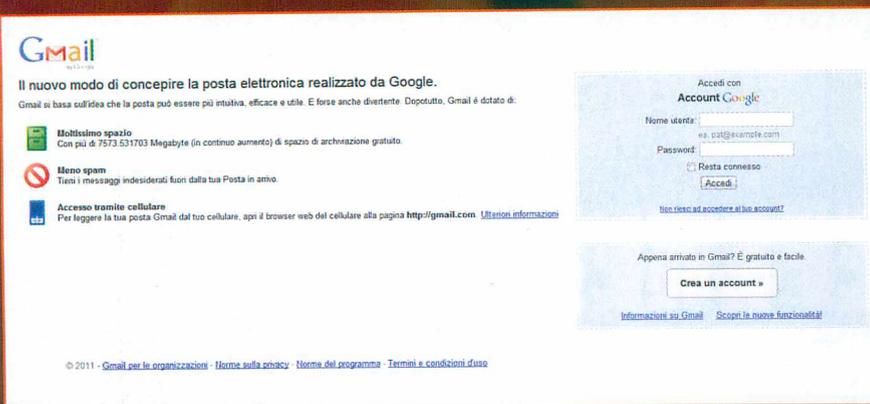
Android in crescita, Chrome OS all'orizzonte, Google Video chiude.

Si è avuta conferma che Google Chrome OS sta superando brillantemente le fasi di test interne e che verrà rilasciato quanto prima da Google. Andrà in concorrenza nel mercato OEM con SO decisamente più anziani, probabilmente collocandosi come concorrente diretto di quel Windows 7 Starter Edition che equipaggia i netbook e che, a sorpresa, si è rivelato essere una scelta vincente per Microsoft. Per ora, però, questo fronte vede Google in crescita presso gli analisti che considerano anche un altro fattore: il mobile è sempre più Android. Impegnare permanentemente i propri avvocati, ultima notizia la denuncia a Samsung per aver copiato funzioni di iPhone, non porta affatto bene a Apple che sente sempre più la pressione del robottino concorrente e lo vede crescere giorno per giorno, affiancato da un Windows Mobile che sembrava quasi nato morto ma sta avendo un suo appeal presso i consumatori. Tutto guadagno per BigG che, aumentando gli investimenti sulla ricerca, conta di sfiancare i concorrenti sull'onda dell'innovazione in tantissimi settori: definire Google un motore di ricerca è ormai un richiamo alla preistoria del Web, visto che BigG si insinua in moltissimi campi tecnologici. Moltissimi ma non in tutti perché, alla fine, anche i giganti possono cedere: Google video chiude definitivamente, con una dichiarazione ufficiale che ha più l'aria di una capitolazione verso YouTube. Una capitolazione tattica: Google Video rappresentava solo un costo mentre YouTube, in cui Mountain View aveva messo lo zampino nel 2006, non ha quasi più concorrenza nel suo segmento.

di Riccardo Meggiato
redazione@hackerjournal.it

E-MAIL ANONIME: SI, NO, FORSE

SI FA PRESTO A PARLARE DI MESSAGGI ANONIMI. LE COSE NON STANNO COSÌ, MA CON UN PICCOLO SFORZO L'INVISIBILITÀ DIGITALE È POSSIBILE.

Sono in molti a riempirsi la bocca di belle parole sull'anonimato della posta elettronica. Beata incoscienza. Uno pensa che basti creare un account fasullo su Gmail per poter imbrattare i forum o, peggio (o meglio, dipende dai punti di vista), inviare allegati contenenti malware, senza essere beccato. Qualcun altro, un pelo più furbo, ricorre ai servizi di invio "anonimo", dove quelle simpatiche virgolette indicano che si tratta di un anonimato un po' farlocco. L'anonimato assoluto, quando si invia una e-mail, è difficile da ottenere, ma scendendo a qualche compromesso possiamo rendere molto difficile risalire al mittente. Diciamocelo: a meno che non si tratti di faccende top-secret come nemmeno ne abbiamo viste con Wikileaks, difficilmente qualcuno si prenderà la briga di inseguirci da un punto all'altro del mappamondo digitale.
Anche se siamo ricercati.
Prima, però, vediamo cosa succede quando inviamo una normalissima e-mail. Semplificando il discorso ai minimi termini umani, il messaggio è trasmesso e preso in carico da un server di posta, che si occupa dell'invio al destinatario. In questo processo, il server conosce perfettamente il nostro indirizzo IP, spesso trasmettendolo così com'è o, in altri casi, mascherandolo. Resta il fatto che se un destinatario ha delle valide ragioni per farlo, può sfruttare la Legge per andare direttamente al sodo, cioè da chi gestisce il server di posta, e chiedergli di sputare il rospo. Risalendo all'indirizzo IP del mittente e, quindi, a noi. Ahia. Molti servizi di anonimizzazione di email tentano di sopperire al problema rendendo il server difficile da individuare. A volte sfruttano dei proxy, rimbalzando il messaggio tra più server sparsi per il globo. In altre, puntano a un unico server, ma locato in paesi non molto collaborativi con le legislazioni del resto del mondo. Di solito si tratta di qualche lontano paese esotico, quindi la scusa di andare a vedere se il server della posta funziona è sempre buona per fare una vacanza al caldo. :-)

Il servizio Gmail? Non ci garantisce l'anonimato. Però, utilizzandolo tramite una VPN, è davvero molto difficile essere smascherati.

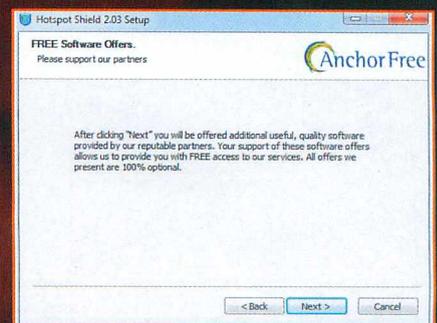
DAL FACILE AL DIFFICILE

Scherzi a parte, dunque, viene spontaneo pensare che un servizio di anonimizzazione della posta offra un buon livello di anonimato. È così? La risposta è "dipende dal servizio", in virtù di quanto detto. Uno dei più diffusi e semplici del momento è Akapost (www.akapost.com).
Si tratta di un servizio di forward che, di fatto, cambia l'indirizzo del mittente con uno ad hoc (scelto dall'utente), in modo che sia questo a comparire al destinatario. Funziona, è gratuito ma le condizioni contrattuali negano utilizzi "nocivi". Il fatto che il gestore sia californiano, comunque, è già un primo, discreto, deterrente ad azioni legali di stampo europeo. A un servizio come Akapost se ne affiancano altri di simili, per i quali è meglio dare un'occhiata alle condizioni contrattuali e, soprattutto, alla locazione. Un deciso passo in avanti lo si fa sfruttando dei servizi di VPN. E in questo caso ce ne sono pochi capaci di battere l'efficienza di Hotspot Shield (www.hotspostshield.com). Questo software gratuito è in grado di creare una Virtual Private Network pronta a rendere imperscrutabili le transazioni web dei nostri dati. E qui viene il bello: Hotspot Shield diventa una comoda base sulla quale poggiare tutte le nostre scorribande tramite posta elettronica. Il trucco, in realtà, è semplice: il problema delle caselle di posta elettronica farlocche, create ad hoc per rimanere anonimi, è che ci identificano tramite un indirizzo IP. Sfruttando un software come Hotspot Shield, invece, il nostro Internet Protocol è mascherato tramite HTTPS, dando filo da torcere a chi vuole arrivare alla nostra identità. Va da sé che basta installare Hotspost Shield, e quindi creare una casella di posta elettronica web, per gestire in modo sufficientemente anonimo le nostre e-mail. Posto che, ovviamente, anche queste devono essere scritte e gestite con la VPN bella che attivata.

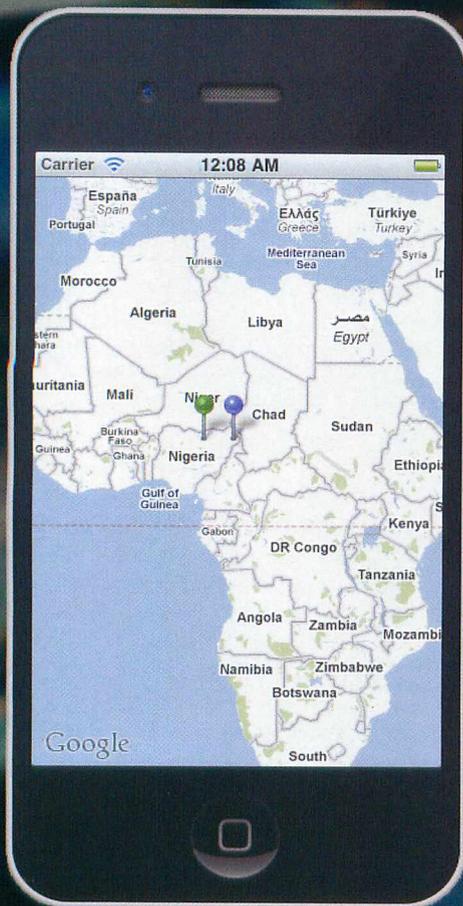
VPN E SMTP SERVER, CHE COPPIA!

L'utilizzo di Hotspost Shield, per altro, apre le porte ad altri utilizzi. Uno dei più ricorrenti, quando si vogliono inviare email anonimi, è di crearsi un proprio SMTP Server. Infatti, se questo server è il primo snodo identificabile per un destinatario deciso a rintracciarci, mascherandolo tramite una VPN la nostra identità rimane protetta in modo efficace. In questo caso, dopo aver installato e attivato Hotspot Shield, passiamo alla creazione di un SMTP Server nel nostro computer. Non è difficile: QK SMTP Server è uno dei programmi migliori nel genere e ripaga ampiamente i 25,52 euro necessari per l'acquisto (e comunque è disponibile una versione dimostrativa gratuita, valida per 30 giorni).
Con una VPN e QK SMTP Server possiamo creare gli indirizzi e-mail desiderati e spedire tutti i messaggi che vogliamo, con un buon compromesso tra semplicità d'utilizzo e livello raggiunto dall'anonimato.

E PER LA POSTA IN RICEZIONE?

Negli ultimi tempi si è sviluppato un grande interesse attorno ai servizi di posta elettronica a tempo, in particolare su 10 Minute Mail (raggiungibile all'indirizzo www.10minutemail.com). Si tratta però di servizi validi per la ricezione di posta, anche se gli indirizzi possono essere sfruttati come "maschere", in fase di trasmissione. Il concetto, in questo caso, è semplice: un servizio che crea indirizzi email temporanei, della durata di appena 10 minuti. Il tempo di mandare qualche messaggio utilizzando questo indirizzo e zzzot... viene eliminato. Risalire al mittente originario diventa molto, molto difficile. Ad accalorare il senso di riservatezza offerto dal sito, ci sono delle condizioni di privacy che garantiscono che non è registrato alcun log delle attività svolte sulle sue pagine. Siamo liberi di crederci o meno ma, in caso contrario, basta utilizzare un proxy o una VPN mentre si visita il sito e il gioco è fatto. Insomma, magari per l'anonimato assoluto serve qualche sforzo in più, ma già con qualche rapido clic si ottiene un'invisibilità informatica difficile da smascherare. Con tanti grazie da parte della nostra privacy.

Hotspot Shield s'installa in pochi secondi e crea una VPN sicura e pronta ad "anonimizzare" tutti i servizi web.

di Salvatore Iaconesi
redazione@hackerjournal.it

INFORMAZIONI GEOREFERENZIATE SULL'IPHONE

AGGIUNGERE CONTENUTI ALLE MAPPE NELLE APPLICAZIONI IPHONE.

Il buffo slogan di un noto operatore di telefonia mobile sembra perfetto non solo per sintetizzare questo articolo di Hacker Journal, ma anche per descrivere un andamento molto comune nelle applicazioni che possiamo scaricare e installare sui nostri smartphone. Tutto intorno a noi...
Le applicazioni location based e, in particolare, la possibilità di posizionare e visualizzare sulla mappa le informazioni che sono attorno a noi, possono essere utili e divertenti, e aprono la possibilità per progettare e realizzare servizi realmente innovativi. In questo articolo vedremo in quali modi possiamo aggiungere informazioni sulle mappe contenute nelle nostre applicazioni iPhone: realizzeremo una piccola App in cui posizionare alcuni contenuti sulla mappa che ne costituirà l'elemento principale. Sul sito Web di Hacker Journal troverete il progetto che potete utilizzare dentro l'ambiente di sviluppo Xcode per compilare e provare questa piccola App.

DA DOVE COMINCIAMO?

Inizieremo quindi col costruire una applicazione base per iPhone su Xcode. Ricordiamo ai lettori che per sviluppare applicazioni per iPhone è necessario iscriversi al sito Apple dedicato agli sviluppatori (http://developer.apple.com) e da lì scaricare l'ambiente di sviluppo Xcode. E' possibile usare alcuni trucchi per sviluppare applicazioni per iPhone usando altri strumenti e piattaforme: magari in un futuro articolo vedremo come ciò sia possibile. Aperto Xcode useremo la funzione "New Project" per creare un nuovo progetto e, scegliendo tra le opzioni disponibili, useremo il template "Window Based Application", tra le possibilità elencate nella sezione iOS. Scegliamo il nome della nostra applicazione ed un luogo sul nostro hard disk su cui salvarla e via, siamo pronti. (Io ho scelto il nome "Posizionami", vedremo che determinerà il nome di alcune classi in Objective-c che ci verranno approntate da Xcode.)

LA MAPPA

Come sappiamo dalla documentazione che Apple mette a disposizione sul sito per gli sviluppatori ogni elemento della nostra interfaccia corrisponderà, nella maggior parte dei casi, ad una sottoclasse della classe *UIViewController* contenuta nel kit di sviluppo di base. Creiamo quindi una sottoclasse di *UIViewController* che conterrà la nostra mappa (la chiameremo *MapViewController*). Dal menu *File* usiamo la funzione "New" e scegliamo l'opzione "UIViewController subclass", selezioniamo "Next" in fondo all'interfaccia, scriviamo il nome e salviamo (cerchiamo di essere il più possibile ordinati e, nel popup che ci chiede dove salvare, mettiamo la classe nella cartella "Classes"). Nel nostro MapViewController, aggiungiamo ora la mappa. Per farlo useremo il MapKit (assicuriamoci quindi che, sull'albero delle risorse di progetto a sinistra dell'interfaccia di Xcode ci siano, nella sezione frameworks, le voci *MapKit.framework* e *CoreLocation.framework* . In caso contrario usiamo la funzione del menu contestuale "Add existing Framework" e selezioniamole dall'elenco). In cima al *MapViewController*, nell'intestazione (il file ".h" della vostra classe), aggiungiamo quindi il supporto per MapKit:

```
#import <MapKit/MapKit.h>
```

Nella interface, definiamo una *MKMapView* usando il comando:

```
MKMapView *map;
```

A questo punto trasformiamo la View in una proprietà della classe, in modo da poterla usare anche da altre classi:

```
@property (nonatomic,retain) MKMapView *map;
```

Poi creiamo un "comportamento" iniziale della mappa e aggiungiamo (nel file ".m" della vostra classe), nel metodo *loadView* che vi viene creato da Xcode quando create una View, i comandi:

```
map = [[MKMapView alloc] initWithFrame:[[UIScreen mainScreen] applicationFrame]];

map.showsUserLocation = YES;

self.view = map;
```

Questi inizializzano la mappa, ne abilitano l'interattività e la aggiungono allo schermo. Ricordiamoci, nel metodo *dealloc* della classe, di rilasciare la memoria occupata dalla nostra mappa tramite il comando:

```
[map release];
```

A questo punto spostiamoci sull'Application Delegate (la classe che gestisce l'esecuzione delle applicazioni iPhone, se avete usato lo stesso nome per l'applicazione si dovrebbe chiamare *PosizionamiAppDelegate*) e aggiungiamo la mappa. Nella intestazione di questa classe importiamo il nostro ViewController tramite il comando:

```
#import "MapViewController.h"
```

A questo punto aggiungiamo la nostra classe al Delegate:

```
MapViewController *mapController;
```

e facciamola diventare una sua proprietà:

```
@property (nonatomic, retain) MapViewController *mapController;
```

Nel corpo dell'Application Delegate (il file .m) usiamo il comando *syntesize* per creare automaticamente i metodi per accedere e scrivere la nostra proprietà:

```
@synthesize mapController;
```

Nel metodo "*application: didFinishLaunchingWithOptions:*" istanziamo la mappa e aggiungiamola alla nostra interfaccia:

```
mapController = [[MapViewController alloc] init];

[window addSubview:mapController.view];
```

ORA COSA CI AGGIUNGIAMO?

Se provate a compilare il codice scritto fin ora, vedrete che l'applicazione funziona e mostra una mappa a tutto schermo. Ora possiamo procedere aggiungendo qualche contenuto. Per aggiungere un elemento alla mappa dobbiamo utilizzare il protocollo *MKAnnotation*. Come suggerisce il nome, questo protocollo è quello utilizzato per gestire le annotazioni sulla mappa. Creiamo quindi una nuova classe (che chiameremo *MyPlaceMark*) usando la funzione "New" e, tra i template, scegliamo di creare una "Objective-C class" e di estendere la classe "NSObject". Modifichiamo il file ".h" di questa classe per fargli implementare il protocollo MKAnnotation, e per aggiungergli un paio di proprietà per contenere un titolo, un sottotitolo e la coordinata geografica dei nostri punti:

```
#import <Foundation/Foundation.h>

#import <MapKit/MapKit.h>

@interface MyPlaceMark : NSObject<MKAnnotation> {
    CLLocationCoordinate2D coordinate;
```

```
        NSString *title;
        NSString *subtitle;
}

@property (nonatomic, readonly) CLLocationCoordinate2D
coordinate;

@property (nonatomic,retain) NSString *title;

@property (nonatomic,retain) NSString *subtitle;

-(id)initWithCoordinate:(CLLocationCoordinate2D)
theCoordinate title: (NSString *) theTitle subtitle: (NSString *)
theSubtitle;

@end
```

Nel corpo della classe usiamo *synthesize* per creare i metodi di lettura e scrittura delle nostre proprietà, diamo implementazione per il metodo di inizializzazione e implementiamo il metodo *dealloc* per assicurarci che la memoria venga rilasciata quando eliminiamo una istanza di questa classe:

```
#import "MyPlaceMark.h"

@implementation MyPlaceMark

@synthesize coordinate,title,subtitle;

-(id)initWithCoordinate:(CLLocationCoordinate2D)
theCoordinate title: (NSString *) theTitle subtitle: (NSString *)
theSubtitle
{
        if( [super init] ){
                coordinate.latitude = theCoordinate.
latitude;
                coordinate.longitude = theCoordinate.
longitude;
                self.title = [theTitle copy] ;
                self.subtitle = [theSubtitle copy];
        }
        return self;
}
-(void) dealloc
{
        [title release];
        [subtitle release];
        [super dealloc];
}
@end
```

Ora abbiamo quindi a disposizione una classe che possiamo utilizzare per ospitare i nostri marker sulla mappa. Ad esempio da codice potremmo usare queste istruzioni per aggiungere un segnale sulla mappa:

```
CLLocationCoordinate2D location;

location.latitude = 12;
location.longitude = 10;

MyPlaceMark *placemark=[[MyPlaceMark alloc]
initWithCoordinate:location title:@"Qui c'è qualcosa"
subtitle:@"Questo è un sottotitolo"];

[map addAnnotation:placemark];
```

Se aggiungiamo, per esempio, questa serie di istruzioni all'inizializzazione della mappa, nel MapViewController, vedremo apparire un puntatore poco sopra l'equatore.

MARKER TUTTI UGUALI

Sarebbe interessante poter personalizzare la rappresentazione dei marker che aggiungiamo alla mappa, ad esempio colorandoli in maniera differente a seconda del tipo di informazione rappresentata.
Per ottenere una funzionalità simile, il SDK di iPhone ci fornisce un altro protocollo, dedicato a configurare la View che viene utilizzata per rappresentare i marker sulla mappa: il protocollo *MKMapViewDelegate*. Per implementare questo protocollo occorre, prima di tutto, aggiungerlo alla definizione della nostra classe MapViewController, in questo modo:

```
@interface MapViewController : UIViewController
<MKMapViewDelegate>
```

Il protocollo ci offre alcuni metodi che vengono invocati quando sulla mappa si verificano eventi o condizioni particolari. E' possibile consultare l'elenco completo di questi metodi nella documentazione di questo protocollo, all'indirizzo http://developer.apple.com/library/ios/#documentation/MapKit/Reference/MKMapViewDelegate_Protocol.
Noi utilizzeremo, in particolare, uno di questi metodi, che viene invocato quando i marker sulla mappa entrano nell'area di visualizzazione:

```
- (MKAnnotationView *)mapView:(MKMapView *)mapView
viewForAnnotation:(id <MKAnnotation>)annotation;
```

Leggendo la *signature* di questo metodo, è possibile comprenderne la funzionalità: fornire una *View* (e, in particolare, una *MKAnnotationView*) dedicata ad una certa annotazione. Procediamo quindi ad implementare questo metodo per personalizzare la vista che viene fornita quando un marker appare sulla mappa.
Iniziamo prima di tutto ad informare il software riguardo a quale classe si occuperà di intercettare questo tipo di chiamate. Come abbiamo visto assegneremo al MapViewController stesso questo ruolo e quindi, subito dopo il codice di inizializzazione della mappa potremo aggiungere l'istruzione:

```
map.delegate=self;
```

Dove *self* in questo caso indica proprio l'istanza della classe controller. Diamo poi implementazione al metodo richiesto dal protocollo:

```
- (MKAnnotationView *)mapView:(MKMapView *)mapView viewForAnnotation:(id <MKAnnotation>)annotation{

        MKPinAnnotationView *vista=[[MKPinAnnotationView alloc] initWithAnnotation:annotation reuseIdentifier:@"myplacemarksview"];

        if([annotation title]==@"Viola")
        {

        [vista setPinColor:MKPinAnnotationColorPurple];

        }
        else
        {

        [vista setPinColor:MKPinAnnotationColorGreen];

        }

        return vista;

}
```

La prima istruzione di questo metodo inizializza la View e la associa all'*Identifier* "myplacemarksview".
Questo è un modo per risparmiare memoria: assegnando tutte le View di un certo tipo alla stessa stringa di identifier potremo far sì che queste vengano riutilizzate (invece che create ex-novo) per rappresentare altri marker che entrino nell'area di visualizzazione.

A questo punto facciamo un piccolo trucco: usiamo il campo "title" della nostra Annotation per decidere che colore assegnare al nostro marker: sappiamo quindi che se il titolo della Annotation dovesse essere la stringa "Viola", il marker sarà colorato proprio di quel colore; in tutti gli altri casi il marker sarà verde. Aggiungiamo quindi un altro marker, vicino al primo che abbiamo aggiunto in precedenza, proprio con questo titolo:

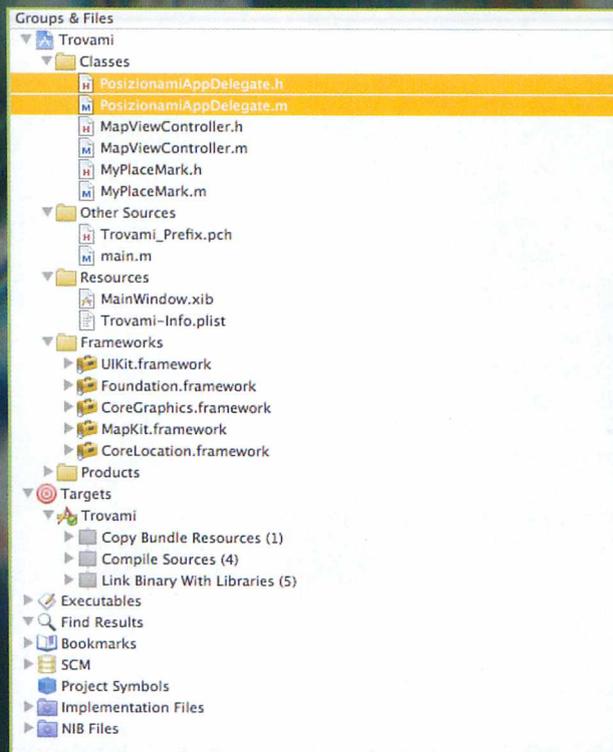
```
CLLocationCoordinate2D locationViola;

locationViola.latitude = 12;

locationViola.longitude = 14;

MyPlaceMark *placemarkViola=[[MyPlaceMark alloc] initWithCoordinate:locationViola title:@"Viola" subtitle:@"Questo è un sottotitolo viola"];

[map addAnnotation:placemarkViola];
```

Eseguendo l'applicazione vedremo quindi comparire un secondo marker colorato di viola.

MARKER DI TUTTI I TIPI

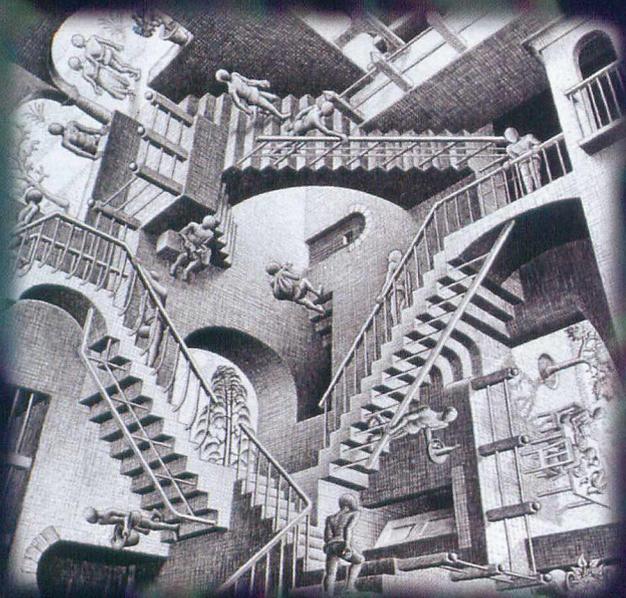
È possibile utilizzare questo metodo per popolare le mappe con marker di ogni genere. Ad esempio possiamo immaginare di creare delle sotto classi della classe *MKPinAnnotationView* per creare animazioni, marker sensibili al tocco o ai gesti, marker video e cose del genere. Basterà in questo caso restituire una istanza della nostra sottoclasse al posto della classe standard e vedremo le nostre mappe automaticamente popolate di marker di tutti i tipi.

IL CODICE E IL PROGETTO XCODE

Associato a questo articolo trovate il codice sorgente ed il progetto Xcode pronto da compilare.
Il codice è molto semplice e potete modificarlo (ad esempio seguendo queste ultime indicazioni sulla realizzazione di marker di tipi differenti) e fare le vostre prove di sistema location based. Vi suggeriamo, ad esempio, di provare a implementare altri metodi del protocollo *MKMapViewDelegate*: alcuni dei metodi che definisce sono utilissimi per personalizzare il comportamento delle vostre mappe, che potranno reagire a tocchi, gesti e condizioni sui dati e sulle informazioni che vi mostrerete sopra.

L'elenco delle risorse utilizzate all'interno del nostro progetto: classi, codice e riferimenti al framework.

di Little Rose
redazione@hackerjournal.it

COME FUNZIONA IL MODELLO EAV?

SULLA CARTA È IDEALE PER ARCHIVIARE DATABASE ENORMI. NELLA REALTÀ VA USATO IL MENO POSSIBILE PER L'IMPATTO SULLE PRESTAZIONI.

Il modello di dati Entity-Attribute-Value viene usato per descrivere entità il cui numero di attributi è potenzialmente enorme ma il cui numero reale risulta relativamente modesto. Matematicamente parlando stiamo facendo riferimento a matrici sparse di grande scala. Un'applicazione tipica del modello EAV è quella delle cartelle cliniche, in cui ogni entità paziente dispone di attributi non standardizzabili per numero e tipologia: data e tipologia di ogni visita, anamnesi, sintomi, esami e risultati e via dicendo. Se decidessimo di usare un DB tradizionale, gran parte dei dati per registrazione sarebbe a null, occupando inutilmente spazio. Il modello EAV, invece, permette di registrare informazioni in una tabella con 3 colonne:

Entità: l'ID dell'entità da descrivere;

Attributo: il nome dell'attributo a cui vogliamo assegnare il valore (definito come foreign key);

Value: il valore da assegnare all'attributo.

Dal punto di vista strettamente teorico, una sola tabella può contenere una quantità di dati impressionante, a patto di referenziare e gestire sia l'elenco delle entità che quello degli attributi oppure di tenere un modello aperto sulle scelte di valorizzazione da inserire. Così facendo, gli elenchi delle identità e degli attributi usati (non quelli disponibili, che vanno referenziati esternamente al modello) è ottenibile con dei distinct. Il problema, semmai, è che il modello non è tipizzato sui valori, non dispone di coppie colonna/attributo e non ha contestualizzazione. Questo significa che l'interrogazione dei dati presuppone una serie abbastanza impegnativa di query sulla tabella-modello che, per sua natura, tende a crescere a dismisura di dimensioni. In più c'è da considerare che l'attributo Value deve obbligatoriamente essere definito in un DBMS come SQL-variant, una complicazione di una certa entità che rende difficoltosa la validazione. Se pensiamo all'insieme di necessità di far funzionare questo modello arriviamo immediatamente alla conclusione che la sola tabella con i dati non basta e servono una serie di meta-data che definiscano il comportamento degli elementi coinvolti: validazione dei valori, insiemi dei valori, gestione delle entità... Suona molto come la definizione di un DB!

FORTI COMPLICAZIONI

Inutile dire che l'utilizzo del modello EAV risulta decisamente più complicato rispetto al modello tradizionale nelle query di selezione e statistica. Immaginiamoci di avere una cartella clinica che contiene i dati anagrafici dei nostri pazienti: data di nascita, peso, ecc. Per selezionare quelli di età superiore a 20 anni e di peso inferiore ai 70Kg con un database relazionale

tradizionale, la query che andremo a scrivere (usando il linguaggio MS SQL Server) sarà simile alla seguente:

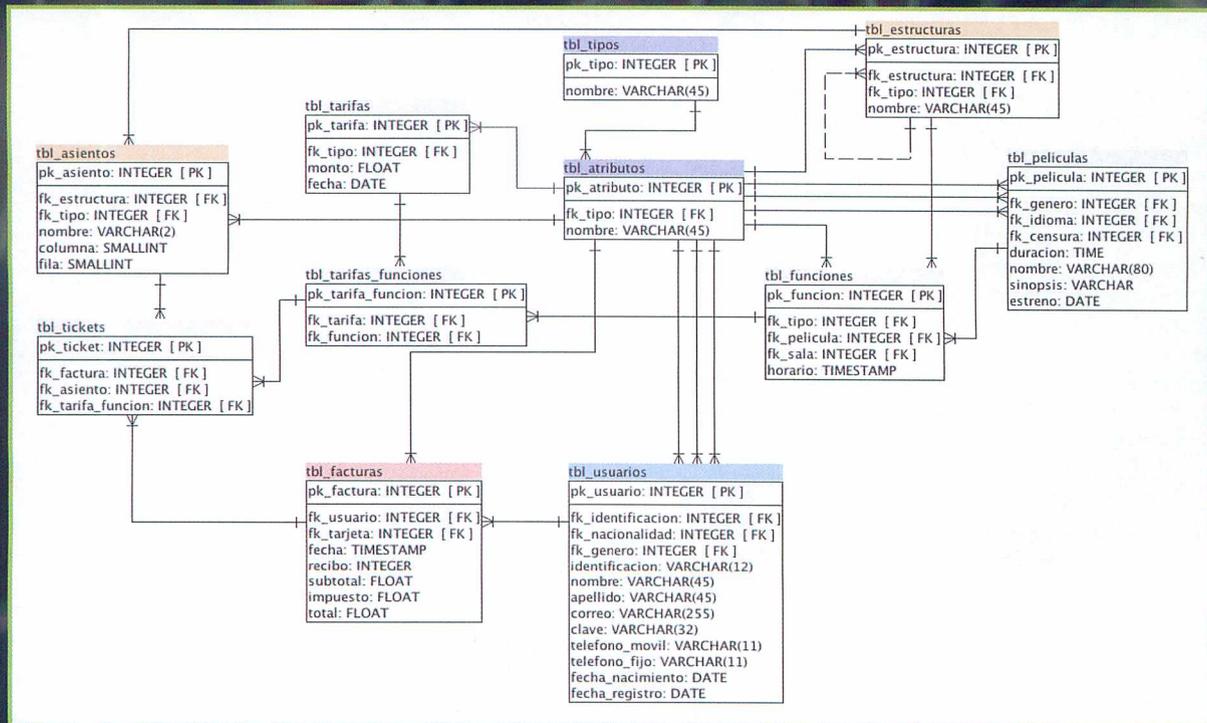
```
SELECT *
FROM Pazienti
WHERE year(now) - year(datadinascita)>=20 and peso<70
```

Ovviamente, dietro, dovremo avere una vista che recuperi l'ultima misurazione disponibile del peso, probabilmente da una tabella Pesi_pazienti che contiene gli ID dei pazienti, la data di misurazione e il peso registrato.
Su un database EAV, sempre usando MS SQL, la query di base assumerà l'aspetto seguente:

```
SELECT pazientiA.pazienteid, pazientiA.valore as Age,
pazientiX.valore as Peso
FROM Pazienti PazientiA
INNER JOIN Pazienti PazientiX ON PazientiX.
pazienteid=PazientiA.pazienteid
WHERE PazientiA.attributo="Age" and PazientiA.
valore>20
AND PazientiX.attributo="Peso"
```

La selezione per due valori, quindi, presuppone un join sulla tabella stessa per il loro recupero e fa solo intravedere la complicazione estrema per cui la selezione di n valori dà vita a n-1 join sulla stessa tabella. Il risultato è che un'applicazione che usi un DB pienamente EAV avrà tempi di coding decisamente più lunghi, una maggiore esposizione a bug e prestazioni notevolmente inferiori a quelle di un'applicazione relazionale equivalente.

PREZIOSISSIMO!

Malgrado gli evidenti problemi prestazionali generali e la complicata gestione, il modello EAV è irrinunciabile in tutti i contesti in cui il numero degli attributi è indeterminato alla progettazione dell'applicazione. Questo, però, non significa che occorre aderire totalmente al modello: possiamo utilizzare un approccio misto che semplifica notevolmente le cose e riduce drasticamente la quantità di meta-dati da gestire a livello del codice. Nell'anagrafica dei pazienti appena vista, alcuni dati di base come il nome e cognome o le date delle visite potrebbero essere inserite in un sistema relazionale, lasciando i dati secondari, oggetto di singole query, in un modello EAV con le entità relazionate al modello tradizionale. Tramite modello relazionale si potrebbero poi definire regole di convalida degli attributi, così da automatizzare anche questo aspetto critico. Il modello potrebbe essere sdoppiato e moltiplicato, così da tipizzare i dati inseriti: ne sono un esempio alcuni DB che hanno una tabella EAV per le date, una EAV per le stringhe, una EAV per i real e così via. Le query risultanti saranno comunque complesse ma certamente i dati verranno validati sfruttando le caratteristiche del DB di supporto e interessando tabelle più sparse. Il modello EAV va quindi usato con una certa attenzione e non deve supplire alla mancanza di analisi dei dati che la nostra applicazione dovrà trattare: ha un utilizzo specifico in contesti dove l'ottimizzazione e la velocità non sono requisiti di base e la sua potenza massima si esprime a supporto di DB relazionali tradizionali.

Uno schema misto tra il modello tradizionale entità-relazione e il modello EAV. Quest'ultimo, da solo, andrebbe evitato come la peste per le problematiche gestionali e le risibili prestazioni.

di G. Enoma
redazione@hackerjournal.it

ANDROID BLACK MARKET

E SE QUALCUNO VI PROPONESSE DI SCARICARE APPLICAZIONI DA UN MARKET ALTERNATIVO?

Ora vi racconto una storia. In effetti non vi dirò se è vera o se è inventata solo per introdurre l'argomento... Sta a voi immaginare.
Tutto nacque il giorno in cui decisi che il mio cellulare aveva proprio bisogno di essere sostituito. Di avventure insieme ne avevamo vissute tante: dal treno ai giri in MTB, dall'aereo al sobbalzare in una cinquecento ("La" 500, quella originale!), alle telefonate a quella che sarebbe diventata mia moglie. Quindi, nonostante i pezzi recuperati dagli amici e la cura con cui avevo tenuto il mio amato Motorola 8700 International, detto amichevolmente "la cabina telefonica", arrivò il giorno in cui fu necessario portarne con me un altro. Dopo "solo" 10 anni dal suo acquisto e malgrado la compagnia della famigerata scheda SIM 5V full-size in dotazione. Ovviamente, un altro cellulare recuperato in casa (che vi credevate? LoL). Col tempo (a dire il vero poco), anche il secondo mostrò tutta la sua obsolescenza e così, dopo solo 2 anni decisi che era arrivato il momento di cambiare. Da buon fedele ai dettami del mondo Open, mi orientai subito verso il robottino verde, tanto più che l'hobby per la programmazione già mi faceva pregustare la possibilità di avere sempre con me le tante applicazioni scritte negli anni, ovviamente dopo un necessario "porting". Scelto marca e modello (un vero e proprio "parto") mi metto in caccia dell'offerta migliore, perché risparmiare non fa mai male. Ho presto scartato tutte le lusinghe degli operatori, che mi sono facilmente suonate tipo quelle televendite "se compri questo fiorellino a 199.99 euro ti regaliamo 6 automobili, un aereo e 3 ville in campagna", con ovviamente (scritta bene in piccolo) la piccola precisazione che se però voglio entrarvi, ci sono qualche milione di euro di abbonamento al possesso delle chiavi...
Ho anche ripassato tutti i mediacenter di elettronica, stranamente allineati (ovvimente verso l'alto) nei prezzi. Poi entro in un negozietto e il titolare mi fa un prezzo per niente di speciale, ma mi dice che mi può fare un deciso sconto in accessori. Mi mostro interessato, dal momento che comunque molti li avrei dovuti comprare. E lui continua: sì, ti posso mettere sul telefonino una serie di applicazioni commerciali senza che tu le debba comprare. Oh oh, la cosa si fa illegale, ma allo stesso tempo gli chiedo di capire di più, perché a noi piace capire. E lì mi spiega che esiste il Black Market, un posto da cui si possono prendere gratis applicazioni che sarebbero a pagamento.
Ho capito: lo ringrazio e vado altrove.

COS'È L'ANDROID MARKET?

Cominciamo dalle cose semplici. Chiunque ha un telefonino con sistema Operativo Android sa che per aggiungergli nuovi programmi basta attivare l'applicazione "Market" e si ha accesso ad oramai più di 100.000 applicazioni pronte per essere scaricate ed installate con un semplice click. Questo è l'Android Market ufficiale. Molte sono gratuite, molte si possono provare, altre vanno comprate. Niente di nuovo rispetto a quanto siamo abituati a fare dal nostro PC. In effetti chi ha un computer con Linux sarà abituato ad avere a disposizione un parco sterminato di applicazioni gratuite, ma l'Android Market non è da meno. Una lieta sorpresa per chi è invece dotato di Windows è il prezzo delle applicazioni Android a pagamento: se comprare un programma per il PC costa per lo meno

importi a due cifre, la maggior parte delle (ottime) applicazioni per i dispositivi con il robottino verde si acquistano tra i 2 e i 9 euro (sì, avete letto bene: da 1,99 a 8,99 – ad essere pignoli).
Si seleziona quella desiderata, si paga con carta di credito (spesso Paypal), un paio di click ed è installata e pronta all'uso.

E IL BLACK MARKET?

Il parallelo con il mondo PC ci continua ad essere utile. Vi ricordate quegli ambulanti con tonnellate di programmi su CD piratati? Recentemente se ne incontrano molti meno, visto che molte delle vendite si sono spostate su Internet, ma sicuramente avrete visto un papà e un figlioletto spulciare le cataste in modo furtivo e poi (credere) di portarsi a casa l'affarone, per pochi euro. Il concetto del Black Market Android è la versione tecnologica e per dispositivi mobili dei sacchi pieni di CD con copertina fotocopiata a cui ho appena fatto riferimento.
Ovvero è un modo per accedere senza pagare ad applicazioni che altrimenti sarebbero a pagamento.
Un po' di cose importanti da chiarire. Un breve "sondaggio" mi ha evidenziato come ci sia una grossa confusione su cosa sia il Black Market. Molti ritengono infatti che sia un sito gestito underground, con URL non pubblicizzato se non tra gli addetti, e magari attivo solo per poco tempo, prima di cambiare. Niente di più sbagliato. Se fate una breve ricerca vi accorgerete che di siti che si fregiano del nome di Black Market... non ce n'è neanche uno(!!!), ma che invece ci sono decine di siti che contengono applicazioni marcate "Black Market". Quindi chiariamo: "Black Market" non è un sito, ma è un aggettivo che può essere assegnato alle applicazioni per evidenziare il fatto che sono distribuite secondo regole diverse da quelle pensate da chi le ha create. Ovviamente ci sono siti che cercano di raccoglierne il maggior numero possibile, categorizzandole, ma questi vanno considerati alla stregua di portali Web. Un link [1] lo trovate nel box, a titolo esemplificativo, e la figura 1 è un esempio di come appaiono.
Ovviamente tenete ben presente che, come per i CD comprati in strada, comprare o scaricare applicazioni messe a disposizione illegalmente è reato. Uomo avvisato...

APPLICATIONS
Books & Reference (14914)
Business (1373)
Comics (1976)
Communication (4243)
Education (3025)
Entertainment (15541)
Finance (3016)
Health & Fitness (3458)
Libraries & Demo (1761)
Lifestyle (9422)
Media & Video (3158)
Medical (925)
Music & Audio (1481)
News & Magazines (4143)
Photography (1476)
Productivity (5204)
Shopping (1836)

Black Market apps for Android
Application's quality filter: All apps
All Free Paid — Sort by Newest Best match Popularity Rating

Lava Lamp Free Live Wallpaper — by Black Market Apps — FREE
Lava Lamp live wallpaper uses real heat transfer physics to create a lava lamp type effect. Lava... black market android

Make It Rain Free — by Black Market Apps — FREE
Make it rain, ya heard!... android black market

Infestation Free LW — by Black Market Apps — FREE
Hope You Got Bug Spray!... blackmarket android

Arachnophobia Free LW (Updated) — by Black Market Apps — FREE
Spiders!!! Get em off me!!! If you like the free version upgrade to... android blackmarket

Android Market Sales Monitor — by Black & White Apps — $1.97

Figura 1. Un esempio di portale per applicazione Android Black Market. Notate che non tutte sono gratis: per alcune si paga una frazione del costo originale.

OCCHI BENE APERTI

Capire le ragioni che stanno dietro alla creazione di una applicazione ABM (sì, accorciamo Android Black Market, tanto ci capiamo) è fondamentale per una scelta corretta delle fonti per le applicazioni da istallare sul nostro telefonino. Su questi siti ne troverete essenzialmente di tre tipi.

Applicazioni semplicemente sprotette. In questa categoria ricadono quelle originariamente a pagamento, che sono state sprotette (qualcuno userebbe il neologismo "crackate") e rese gratuite da qualcuno che tipicamente crede nella circolazione libera delle idee e a cui non va giù che un programma debba essere pagato. Siccome la motivazione (condivisibile o no) è puramente ideale, l'unico rischio è collegato con l'illegalità dell'atto.

Applicazioni sprotette e rivendute a prezzo inferiore. Qui troviamo i furbetti: coloro che agiscono per fare soldi alle spalle di chi ha creato il prodotto. Di fatto rimettono in vendita ad un prezzo inferiore applicazioni che sarebbero più costose. La motivazione è "fare soldi facili" e questo sembrerebbe poterci far stare tranquilli. In realtà chi vuole fare soldi facili non si accontenterà dei pochi euro che gli date esplicitamente, ma avrà pensato magari ad altri modi meno trasparenti. Ad esempio potrebbe voler rivendere il vostro indirizzo di e-mail (quello usato durante la transazione), oppure aggiungere moduli per tracciare la vostra navigazione e vendere l'informazione.

Applicazioni sprotette e modificate, rese disponibili gratis. Si tratta di una variante del primo caso, in cui apparentemente non c'è nulla da pagare. Tuttavia chi le mette in circolazione ha intenzione di fare soldi facili, alle vostre spalle.
Per fare un piccolo esempio preso dal mondo PC, come pensate che le principali organizzazioni criminali di Internet costruiscano le loro reti di centinaia di migliaia di nodi Zombie sparsi ai quattro angoli della Terra?
Se chi agisce non è mosso da ragioni ideali, nessuno regala niente per niente, e noi non abbiamo modo di conoscere le ragioni di qualcuno che non possiamo nemmeno vagamente identificare.

APKTOR

Se a questo punto siete ancora decisi a capire di più sull'Android Black

Figura 2. L'interfaccia dell'Applicazione APKtor, un enabler per l'accesso diretto ad applicazione di tipo Black Market.

Market vi sarete sicuramente chiesti come si fa a dire al nostro telefonino di puntare a uno (o più) siti "Black". Ovviamente una prima possibilità è quella di raggiungere l'applicazione desiderata via Web, ovvero tramite uno dei portali a cui facevo riferimento. La si scarica e la si installa come fareste sul PC per qualunque applicazione trovata su Internet. E poi sui siti ci sono comunque le istruzioni relative.
Ma per coloro per cui tutti questi passi sono comunque faticosi (ho visto dita sudate annaspare sugli schermi touch e chiedere il pensionamento anticipato) sarebbe comunque bello avere una funzione simile all'icona Market (quella che ci punta alla repository ufficiale Android) anche per l'ABM.
A costoro viene incontro una semplice applicazione OpenSource chiamata APKtor [2].
Al momento in cui scrivo, l'ultima versione è la 1.0.8.7. Notate che APKtor lo trovate sul Market ufficiale, ed il suggerimento è di installarlo da quella fonte (sono solo 150 KB).
Per farla funzionare, dopo esservi accertati di avere il WiFi attivo e di essere effettivamente connessi, attivatela e andate nel menu "Repositories". Qui dovete inserire la lista dei siti ABM che volete che APKtor scansioni. A questo punto dovete aspettare che la lista si aggiorni (potrebbe volerci un po'). Come potete vedere dalla figura 2, l'interfaccia è molto pulita e ben fatta e si spiega veramente da sola.

CONSIDERAZIONI FINALI

La cultura hacker ci suggerisce di non esprimere giudizi, ma solo di cercare di capire e poi divulgare la conoscenza acquisita, sviluppando in ciascuno quel sano spirito critico di cui c'è tanto bisogno nel mondo. Vorrei quindi farvi riflettere su alcune domande che io mi sono posto.
Io sono uno sviluppatore (per hobby) e so quanta fatica costa sviluppare programmi ben fatti, facili da usare, ben documentati, veloci e (il più possibile) bug free. Per me è un hobby, ma capisco che se qualcuno ci deve campare avrebbe due strade: tenere i prezzi alti, magari a scapito dei volumi, sperando nella necessità del mercato, o puntare sul lungo termine, tenendo i prezzi bassissimi e puntando su grandi volumi. Nel mondo PC i produttori hanno puntato alla prima strada, mentre nel caso Android, il mercato si è decisamente orientato per la seconda.
Se ora mi metto nei panni dell'utente, posso trovare giustificazioni per boicottare il comportamento speculativo del mercato per PC, ma quali ragioni posso trovare per non dare 2 euro (fossero anche 4) a chi ha speso centinaia di ore per fare qualcosa che giudico buono?
La seconda domanda sorge più dal mio lato professionale, ovvero l'analisi dei rischi. Nella mente di chi usa gli smartphone essi sono ancora considerati immuni da rischi di tipo informatico. Molti li vedono infatti ancora come semplici telefonini, a cui "che danno vuoi che si possa fare?". In realtà gli smartphone sono oramai veri e propri computer con capacità di calcolo, memorizzazione e connettività non inferiori a dispositivi IT più tradizionali. Hanno un sistema operativo e possono ospitare qualunque tipo di malware. In più, sullo smartphone tendiamo a salvare moltissime informazioni sensibili, spesso senza neanche farne una copia al di fuori del telefonino stesso. Con questa premessa, mi sono chiesto: quanti euro vale il rischio di infettarsi, perdere dati importanti e/o la nostra privacy? Scaricare un'applicazione modificata da un estraneo qualunque (probabilmente animato da secondi fini) invece di quella supportata è come aprire la porta e dare le chiavi di casa senza sapere chi vuole entrare e perché... E tutto ciò per risparmiare 4 euro? Ciascuno di noi ha sicuramente modi più salutari e meno rischiosi di risparmiare.
Cosa succede quando l'applicazione originale viene aggiornata?
Non è affatto detto che il nostro "pirata" la aggiorni per incorporare le nuove funzioni e ereditare (magari) una versione in cui le falle di sicurezza che lui aveva usato per sbloccarla sono state chiuse.

La scelta finale sta comunque a voi: con questo articolo spero di avervi passato le informazioni per una decisione informata e consapevole. Ricordate: la conoscenza è un potere, e va usata bene.

PER APPROFONDIRE

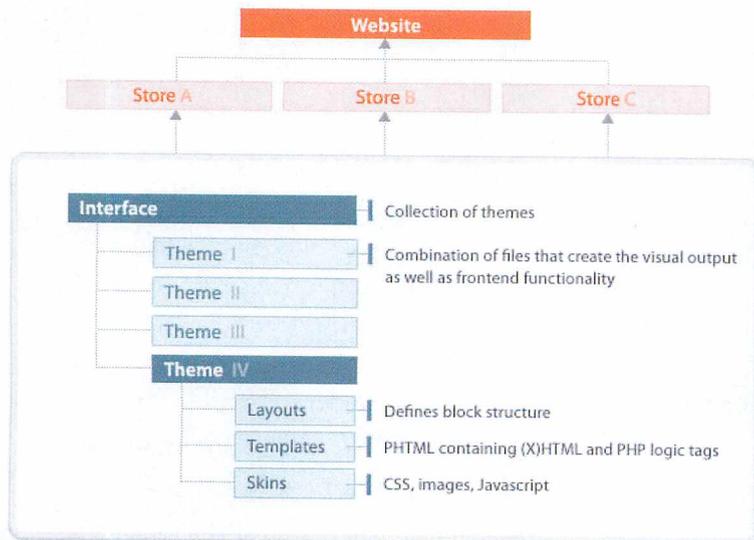
Qui di seguito i link alle informazioni referenziate o utilizzate nella stesura dell'articolo, e qualche altra fonte utile:

[1] http://www.androidzoom.com/android_applications/black%20market

[2] APKtor: Questa applicazione è sul Android market ufficiale, ma non la trovaste, un link alternativo è: http://www.tactools.org/apktor-v1-0-8-7-google-android-black-market.html

http://bubbleandroid.com/android-black-market-free-apps/

di M45t3R EWS
redazione@hackerjournal.it

ARCHITETTURA DI MAGENTO

LA PIATTAFORMA DI E-COMMERCE PIÙ DIFFUSA È OPEN SOURCE E UN ESEMPIO DI MODULARITÀ DA SEGUIRE.

MAGENTO SU CD

La versione Community Edition di Magento è disponibile come programma sul CD di Hackers Magazine numero 67.

Magento (www.magentocommerce.com), attualmente, sembra essere la piattaforma di e-commerce più diffusa, con oltre 90.000 installazioni funzionanti, oltre 3 milioni di downloads e 25 miliardi di transazioni gestite annualmente. Sfruttando lo Zend Framework (framework.zend.com) offre un ecosistema integrato a rapido sviluppo di applicazioni per la vendita online dei prodotti più vari: dalle auto alle creme passando per gli alimentari e i prodotti tessili. Basato sullo Zend Framework, offre l'indubbio vantaggio di fornire un motore perfettamente funzionante e totalmente configurabile su cui innestare temi grafici ma anche plugin (oltre 3500 quelli già disponibili) che possono intervenire ad ogni livello dell'applicazione: dalla fornitura di dati in real time sulle disponibilità del magazzino alla gestione dei buoni sconto, dalla possibilità di fare offerte di prodotti mirati a target specifici all'interfaccia con i più diffusi sistemi gestionali. Il suo funzionamento e le sue possibilità di personalizzazione si basano su un'architettura a template programmabili divisa in tre aree:

/app/design/frontend/default/<template_name>/layout/
Contiene i file XML che verranno intepretati dal Core di Magento per l'inclusione dei file del template;

/app/design/frontend/default/<template_name>/template/
Contiene tutti i file necessari per processare il template;

/skin/frontend/default/<template_name>/
Contiene tutti i file non programmabili del template: immagini, file CSS, contenuti Flash, javascript e via dicendo.

Ciascun template viene poi organizzato in due livelli distinti, come le buone tecniche di programmazione insegnano: blocchi strutturali e blocchi di contenuto.

I primi vengono usati per organizzare le pagine mentre gli altri per fornire i contenuti di cui fare il rendering. Ciascun blocco strutturale, poi, definisce autonomamente i suoi propri contenuti per il rendering, inserendo parti provenienti da funzioni del sistema, da funzioni programmate su misura o da blocchi statici. Il risultato è quello di poter isolare nel dettaglio ogni parte delle pagine da elaborare, fornendo una flessibilità di impaginazione enorme e garantendo l'isolamento dei componenti di codice. Basta ricordarsi di rispettare sempre la struttura di base perché l'inserimento di codice in moduli casuali può rendere piuttosto difficoltoso qualsiasi debug.

Lo scotto da pagare per avere tutta questa flessibilità sta nel flusso di elaborazione del rendering fatto dal Core di Magento. Questo carica innanzitutto tutti i blocchi di struttura interessati dal layout del sito e li processa singolarmente. Per ognuno di questi va a recuperare i contenuti definiti dai blocchi di contenuto, in modo autonomo. Il risultato viene assemblato pezzo per pezzo e poi passato all'utente finale come pagina completa. Considerando che ogni layer può rimandare ad altri dello stesso livello (in un sistema ricorsivo), è facile capire come il procedimento metta sotto stress le risorse della macchina che ospita il sito. D'altra parte, il Core sfrutta automaticamente una serie di cache proprio sui contenuti e sulla struttura che gli permettono di evitare di recuperare informazioni già preparate in precedenza per il rendering.

DAI FILE XML ALLA PAGINA

Per assegnare i blocchi di contenuto ad ogni blocco di struttura, Magento processa una serie di file XML a partire dal loader di default: page.xml. Questo include una serie di altri XML, così che è piuttosto facile espandere il sistema: basta identificare il file XML che controlla la parte da modificare e aggiungere i riferimenti al nostro blocco personalizzato. La struttura tipica di un XML di definizione del blocco è la seguente:

```
<default>
<reference name="header">
<block type="page/html_header" name="header"
as="header">
<block type="page/template_links" name="top.links"
as="topLinks"/>
<block type="page/switch" name="store_language"
as="store_language" template="page/switch/languages.
phtml"/>
<block type="core/text_list" name="top.menu"
as="topMenu"/>
</block>
</reference>
</default>
```

A causa della sua modularità, il flusso di rendering di Magento è tutt'altro che lineare. Per fortuna vengono gestite ottimamente delle cache ed evitate rielaborazioni continue.

L'uso di XML non ci induca a credere che Magento offra layout statici, perché il Core ci mette a disposizioni anche blocchi funzionali che permettono di decidere quali parti proporre al client in runtime come blocchi if (usati, per esempio, per distinguere i browser: <if>lt IE 7</if>). Lo stesso vale per l'aggiunta di parametri e personalizzazioni riguardanti CSS, Javascript e tutto il contenuto aggiunto della pagina, con blocchi simili al seguente:

```
<action method="addCss">
<stylesheet> css/print.css </stylesheet>
<params> media="print" </params>
</action>
```

Nel dettaglio, i tag utilizzabili insieme a method vengono processati come array e possono, quindi, essere concatenati e ampliare le possibilità di modifica dei contenuti: con un solo comando action possiamo sopprimere un contenuto oppure aggiungere in concatenazione altri blocchi. Una guida a queste funzioni è disponibile all'indirizzo www.magentocommerce.com/design_guide/articles/intro-to-layouts.

GERARCHIE

Caratteristica che ha fatto di Magento uno strumento potente dal punto di vista dei programmatori è il funzionamento del Core in via gerarchica. Qualsiasi elemento richiamato da page.xml o dagli xml successivi viene cercato in una serie di directory per poi andare in fallback sul tema default, presente in ogni installazione. Questo impedisce la maggior parte dei problemi che si riscontrano con un'organizzazione così frammentaria delle pagine e, collateralmente, permette di ottenere siti personalizzati semplicemente creando un tema secondario vuoto e inserendo al suo interno gli elementi grafici che si desidera sostituire. Questo meccanismo, inoltre, non si applica solo agli oggetti di contenuto ma anche a tutti gli XML di layout,

L'interdipendenza di ogni modulo che compone il Core di Magento è elevatissima. Per fortuna, grazie alla sua struttura, Magento può essere personalizzato poco per volta.

permettendo di inserire modifiche su temi già pronti tenendo distinte le rielaborazioni dagli originali.

IL CODICE

La struttura gerarchica sfruttata per i layout viene usata anche per il codice che fa funzionare tutto il sistema, raggruppato nella directory /app/code/. Questa contiene tre sotto directory in cui il codice viene suddiviso, corrispondenti ai tre layer di fallback usati. In fase di programmazione, questa divisione va rispettata rigorosamente per evitare confusioni nel debug.

Core

Ospita il Magento Core e non bisognerebbe mai modificare alcun file contenuto al suo interno perché ogni aggiornamento di Magento va a sovrascrivere tutti i suoi contenuti. È il livello di fallback più basso.

Community

Raggruppa le estensioni installate tramite le funzioni Magento-Connect (in modo automatico) oppure scaricate e installate manualmente. Va a sovrapporsi a Core nel fallback. Le modifiche manuali di queste estensioni sono scoraggiate perché interferiscono con i meccanismi di aggiornamento delle estensioni ufficiali.

Local

Strato più alto nel meccanismo di fallback, questa directory è preparata per ospitare le estensioni su cui stiamo lavorando oppure quelle che funzioneranno esclusivamente sulla macchina su cui stiamo lavorando.

Questo approccio permette di recuperare un modulo da Core, copiarlo in Local, modificarlo e vederlo in funzione senza dover alterare nulla della struttura di base dell'applicazione. Un vantaggio notevole quando l'applicazione in questione è composta da decine di moduli Core che interagiscono continuamente tra loro. Ogni modulo, di qualsiasi livello sia, è inoltre strutturato per mantenere le caratteristiche di divisione del codice e integrazione tipiche di Magento. Osservando i vari moduli disponibili nel Core stesso, noteremo una directory Block che contiene i processori di rendering del modulo, chiamati dagli XML di layout. Da notare la presenza di una directory sql contenente gli script MySQL da eseguire all'installazione e alla disinstallazione del modulo in questione. Il richiamo del blocco avviene tramite gli XML che vengono integrati nella cartella /app/design/frontend/<interface>/<theme>/<layout>/<example>/.

ZEND?

L'intero sistema Magento è basato sul framework Zend, che fornisce le classi di base necessarie per qualsiasi funzione di basso livello, con un'operazione che ha portato l'azienda che l'ha creato (Varien) a costruire uno strato superiore a quello offerto dal framework per la gestione del lato e-commerce. Questo rende l'utilizzo e la personalizzazione di Magento un problema relativamente semplice per chi ha già un'esperienza con strumenti Zend based.
Per tutti gli altri, il consiglio è quello di partire proprio dal download dello Zend Server CE (www.zend.com/en/community/pdt) e dalle basi del framework prima di affrontare la strutturazione di applicazioni Magento perché, addentrandosi nel sistema, ci si trova ad avere a che fare con codice PHP completamente OOP: un trauma per chi non ci è più che abituato.

COSA SERVE

Per far girare Magento serve come minimo un daemon Apache con PHP 5.2.13 (esteso con PDO_MySQL, simplexml, mcrypt, hash, GD, DOM, iconv, curl, SOAP), almeno 256 Mb di memory limit, Safe mode a off e MySQL 4.1.20 con InnoDB.

Se abbiamo il sito in hosting, assicuriamoci di avere il controllo del crontab con PHP5 e di poter gestire le opzioni in.htaccess. Ovviamente, il SO principe per far girare tutto questo è Linux, anche se alcuni sono riusciti a installare e a far funzionare Magento in ambiente di test WAMP.

Per lo sviluppo possiamo usare Eclipse, visto che Zend ci fornisce il PDT, aggiungendo, magari, Zend Server Community Edition (www.zend.com/en/products/server-ce/downloads).

di Andrea Draghetti
redazione@hackerjournal.it

RSA Security è una divisione della EMC Corporation fondata nel 1982 con l'intento di progettare i migliori sistemi di protezione di dati personali ed aziendali, e il nome deriva dall'omonimo sistema crittografico creato nel 1976 dai due famosi ingegneri e crittografi Whitfield Diffie e Martin Hellman.

UN FURTO MISTERIOSO E LA SICUREZZA DI MILIARDI DI TRANSAZIONI È A RISCHIO.

SONO FAMOSI

Il loro prodotto più diffuso è sicuramente la SecurID , ovvero una chiavetta OTP (One Time Password) sfruttata principalmente per l'accesso online agli Istituti Bancari ma anche alle infrastrutture aziendali. La SecurID genera una password composta da sei numeri ogni sessanta secondi e visualizzabile attraverso un piccolo schermo, solitamente LCD, posto sulla chiavetta. Il funzionamento dei SecurID si riassume attraverso i seguenti tre elementi.

RSA Authentication Manager: verifica i dati immessi dall'utente;

RSA Agent: si installa sulle risorse da proteggere, creando un sottolivello di sicurezza che permette il colloquio con l'Authentication Manager;

Tokens: genera i codici numerici, detti *Tokencode*, sincronizzati temporalmente con l'Authentication Manager.

Durante la fase di login l'utente dovrà digitare il Tokencode visualizzato sul display della chiavetta, il quale dovrà corrispondere a quello generato dal RSA Authentication Manager; se i dati corrispondono, RSA Agent procede ad abilitare l'utente consentendoli l'accesso alle risorse richieste. Importante precisare che per il corretto funzionamento il token e il server devono essere perfettamente allineati con il clock UTC, così facendo calcoleranno nel medesimo istante lo stesso codice.

Art Coviello, Chief Executive Officer della RSA, attraverso un comunicato stampa, ha reso noto che la propria società è rimasta vittima di un sofisticato atto informatico finalizzato

Tutte le banche permettono di avere un conto online e tutte, nel mondo intero, usano i dispositivi (brevettati) prodotti dalla EMC.

al furto di dati sensibili e del tipo APT (Advanced Persistent Threat), per colpire l'azienda è stato effettuato un Spear Phishing collegato ad una falla 0-Day di Adobe Flash Player.
Lo Spear Phishing non è un attacco generico di Phishing ma è mirato ad un obbiettivo ben preciso e lascia intendere che il mittente sia una persona conosciuta (amico, famigliare, collega o datore di lavoro) abbassando notevolmente la guardia del bersaglio. In realtà le informazioni sul mittente vengono falsificate o ricavate tramite "spoofing", mentre il phishing tradizionale si propone di sottrarre informazioni da singoli utenti. Le frodi che si basano sullo spear phishing hanno come obiettivo quello di penetrare all'interno del sistema informatico di una società e realizzare un attacco di tipo APT.
Un attacco in grande scala.
Uri Rivner, capo delle nuove tecnologie della RSA, ha rilevato nel suo Blog che l'attacco è accaduto principalmente in tre fasi.
Nella prima fase l'attaccante ha inviato a due piccoli gruppi di dipendenti una eMail con oggetto "Piano di Assunzioni 2011" contenente un file Excell, un dipendente incuriosito ha aperto l'allegato il quale realmente conteneva un malware che ha sfruttato la falla 0-Day di Adobe Flash Player per installarsi sul terminale. Successivamente l'attaccante ha iniziato la scalata verso gli account più importanti della RSA Security, sfruttando il terminale compromesso ha rubato credenziali di accesso e si è propagato a macchia d'olio in tutta l'infrastruttura aziendale. Sembrerebbe che le credenziali d'accesso di ogni singolo utente siano utilizzabili su molti terminali della società e non esclusivamente nel terminale in uso dal dipendente, questo ha permesso all'attaccante di identificarsi con le credenziali dell'utente di basso livello (dipendente) nei terminali dei diversi responsabili aziendali rubando ulteriori password e materiale importante. Materiale che risulterebbe ancora non identificato.
La terza e ultima fase ha visto l'invio di tutti i documenti rubati ad un computer esterno presso un Hosting Provider, in precedenza violato, dal

L'OTP della RSA Security è talmente diffuso che l'azienda si identifica con esso. Il prezzo del monopolio globale di questa tecnologia.

quale l'attaccante ha recuperato i dati eliminando quasi tutte le tracce. Brian Krebs, famoso giornalista Americano sul CyberCrime, ha dichiarato che sarebbero stati identificati tre indirizzi IP sfruttati per l'intrusione, uno dei quali proveniente dalla P.r.C. (People's Republic of China), ma ovviamente potrebbe essere stato uno stratagemma per rallentare le indagini.

UN FURTO MISTERIOSO

Ad oggi però non conosciamo esattamente cosa sia stato sottratto dai sistemi informatici della RSA; i giornali più distratti hanno reso noto il furto dell'algoritmo, ma essendo pubblico dal 2000 è piuttosto facile rubarlo :-) Piuttosto è possibile che sia stata trafugata una Master Key. Infine non dimentichiamoci che la RSA Security non produce esclusivamente SecurID. Il furto potrebbe riguardare tutt'altro anche un semplice database con l'archivio dei clienti. È stato proprio Whitfield Diffie ad ipotizzare il furto della Master Key ossia una stringa molto grande, utilizzata come parte integrante dell'algoritmo presente nei server di Authentication Manager. Attraverso la Master Key nei peggiori dei casi l'attaccante riesce a riprodurre dei Tokens gemelli a quelli originali, rendendo così più facile l'accesso ad un sistema informatico protetto. Questo avvenimento, che ha colpito una delle più imponenti aziende di Sicurezza Informatica, ci insegna che non dobbiamo mai abbassare la guardia nemmeno da una eMail inviataci dall'amico di infanzia e soprattutto apportare una corretta politica di IT Security all'interno delle aziende, includendo nei corsi tutte le persone che quotidianamente usano un terminale e addestrarli ad evitare un attacco di Ingegneria Sociale che è sicuramente il sistema più diffuso per rubare informazioni importanti.

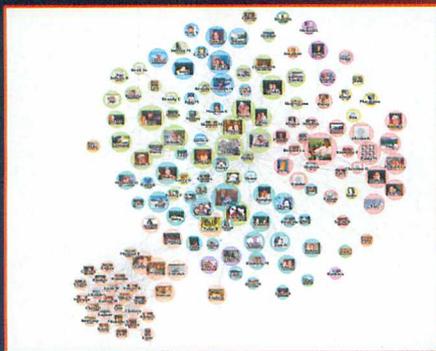
di Riccardo Meggiato
redazione@hackerjournal.it

CONDIZIONARE L'OPINIONE PUBBLICA? GLI USA POSSONO

SCOPERTO UN PIANO DEGLI USA PER LA CREAZIONE DI FALSI PROFILI NEI SOCIAL NETWORK, IN MODO DA INFLUENZARE LE OPINIONI DEL POPOLO WEB.

Un codice identificativo, RTB220610. Di lui si sa poco, anzi pochissimo. Sembra essere passato sotto gli occhi di tutto il popolo americano, senza sortire alcuna reazione. Poi, un bel giorno, qualcuno decide di dare un'occhiata alle gare d'appalto dello U.S. Air Force, una delle più potenti strutture militari del mondo. E fa la scoperta. Il codice corrisponde alla richiesta di sviluppo di un software, per la precisione un Persona Management Software. Il suo scopo? Presiedere al funzionamento di un Online Persona Management Service, che tradotto in parole povere equivale a un sistema per la gestione di "persone". Non nel senso fisico, in carne ossa, ma nell'equivalente digitale. Profili, insomma. Profili online. Anche detta così, la situazione sembra normale, perché la gestione di profili digitali è quanto di più generico si possa sentire in ambito web di questi tempi. Qualsiasi social network gestisce profili, in ogni istante. Ma, banalmente, anche un qualunque sistema di gestione del personale lo fa, specie nelle grandi aziende, con gli account dei dipendenti. Ma il Persona Management Software voluto dall'alto comando americano è qualcosa di dannatamente più complesso, misterioso e, ahinoi, pericoloso. Si parla di profili di social network, e l'intenzione non è certo quella di promuovere l'utilizzo di Facebook tra i militari. Tutt'altro.

UN BANDO MOLTO MISTERIOSO

Il bando di concorso, disponibile pubblicamente all'indirizzo www.seankerrigan.com/docs/PersonaManagementSoftware.pdf, parla di una richiesta di 50 licenze software, ciascuna delle quali deve essere in grado di gestire fino a 10 "persona". Un utente, e quindi una licenza, dieci profili. Cinquanta licenze, cinquecento profili. In pratica, un gruppo di 50 dipendenti dello U.S. Air Force devono essere in grado di gestire, tramite il Persona Management Software, uno squadrone di 500 profili digitali. La richiesta parla chiaro sulle specifiche di queste "persone" virtuali: "software will allow 10 personas per user, replete with background, history, supporting details, and cyber presences that are technically, culturally and geographacilly consistent". Che tradotto significa "il programma assegnerà 10 profili per utente, complete di background, storia, dettagli e presenze virtuali che siano tecnicamente, culturalmente e geograficamente consistenti". Ogni persona digitale, dunque, deve essere credibile. E si continua: "Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms". Ossia: "le persone digitali devono sembrare provenire da qualsiasi parte del mondo e devono poter interagire

Un semplice giochino di Facebook. Quante informazioni può contenere su di noi e sulle nostre idee?

tramite i convenzionali servizi online e le piattaforme social media". Insomma, in parole povere, i profili digitali devono sembrare originali e gestiti ciascuno da un vero proprietario in carne e ossa.

RICHIESTE POCO CHIARE

Il bando di concorso continua con i dettagli, che vanno oltre il software primario. Per esempio, si richiede la costituzione di una rete Virtual Private Network in grado di garantire che, a rotazione, a ogni utente sia assegnato un indirizzo IP generato casualmente, per rendere ancora più credibile l'operazione. Del resto, al punto successivo, è richiesta anche la possibilità di assegnare un indirizzo IP statico a ogni persona virtuale. Questo per far credere, recita testualmente il documento, che un profilo risulti di proprietà della medesima persona nel corso del tempo. Tra le altre richieste, come ciliegina sulla torta (si fa per dire), la possibilità di far sembrare autentica e ben georeferenziata la provenienza di un profilo digitale. Da questo quadro complessivo emerge che l'Online Persona Management Service ha uno scopo ben preciso: gestire profili falsi, ma credibili, pronti ad apparire nel mondo dei social network come alter ego di utenti reali. Il bando, tuttavia, non rivela quale possa essere il fine ultimo di un'operazione di questo tipo. E dunque, dopo la scoperta, inizia il tam tam. E a infittire il mistero giungono, guarda caso, una serie di email materializzatesi come per magia: si tratta di una fitta corrispondenza di documenti legati al progetto, da parte della società di sicurezza HBGary. Da questa documentazione emergono diversi nuovi e scottanti dettagli.

TANTA (TROPPA) VOGLIA DI SOCIAL NETWORK

Innanzitutto, il sistema di Online Persona Management Service serve a creare "amicizie" virtuali tramite i social network, da sfruttare per ottenere informazioni su determinati individui. Gli obiettivi sono, essenzialmente, Facebook, Twitter e MySpace, ma si lasciano aperte le porte anche a interazioni con altri servizi online. L'idea è di creare degli archivi di dati altrui per ottenere credenziali sociali sempre più elevate, sfruttandole col social engineering per avere informazioni sempre più personali. Come rivelano le email scovate, l'intento è di raggiungere anche gli individui più protetti e informaticamente introversi, partendo da dati quali la città di provenienza e la scuola frequentata. Sulla base di questi, per esempio, ci si iscrive a un sito come classmates.com, venendo a conoscere compagni del soggetto non iscritti a Facebook. E così si creano i loro (falsi) profili, ottenendo l'amicizia desiderata. Muovendosi velocemente, l'individuo sotto controllo non ha nemmeno il tempo di accorgersi di avere a che fare un profilo fasullo, e si ottiene una miriade di informazioni utili. Per esempio la lista di amici, tra i quali si possono conoscere nuovi obiettivi. Stringendo amicizia con questi, si innestano altri possibili catene di contatti, a cascata. È solo un piccolo esempio di ciò che si può fare con un profilo falso. Immaginiamoci, ora, cosa è possibile fare con un "esercito" di 500 persone virtuali. Con queste si creano network immensi di contatti, e dopo una fase di footprinting, cioè di raccolta di informazioni, si può passare a una strategia decisamente più attiva: la temibile propaganda digitale.

I social network sono già un pericolo per la privacy: se ci si mettono anche gli stati conviene abbandonarli.

PROPAGANDA! PROPAGANDA!

In cosa consiste? In effetti se ne sente ancora parlare poco, ma è vista come la nuova frontiera del social engineering. In pratica, sfruttando un corposo network di falsi profili, si inviano messaggi facendoli passare come una moda o una volontà popolare. Per esempio la preferenza nei confronti di un candidato alle elezioni. O, perché no, la "conferma" di voci relative a scandali inesistenti. Pensiamo che accadrebbe se 500 profili Facebook iniziassero una propaganda diffamatoria nei confronti di un politico, per esempio accusandolo di pedofilia. Si scatenerebbe una vera e propria gogna mediatica pronta a incolpare un individuo magari innocente. Estendendo il concetto alla politica estera, una propaganda di questo tipo potrebbe dare il "la" a delle rivolte popolari nei confronti di un governo ostile. La miccia pronta a scatenare delle rivoluzioni. È un po' il concetto che sta dietro ai flash mob, se vogliamo, anche se con finalità e ripercussioni ben diverse. Il punto è che l'Online Persona Management Service è un progetto avallato dal governo americano, e pronto a entrare presto in azione. Come e quando non si sa, e ovviamente sarà difficile rendersene conto, resta il fatto che i social network, una volta di più, andranno presi con le pinze.

di penelope.di.pixel
redazione@hackerjournal.it

ZERO DOLLAR LAPTOP

UNA STORIA (VINCENTE) DI ACCESSO RADICALE.

La storia di questo progetto inizia nel marzo del 1999 ad Amsterdam durante la conferenza ***The Next 5 Minute*** quando James Wallbank, coordinatore della ***Redoundant Technology Initiative***, espone ad un audience di new media e attivisti il ***Lowtech Manifesto***. Si tratta di un documento agile e sintetico, ma capace di colpire nel segno e di individuare una tendenza: l'industria spinge i consumatori ad acquistare laptop, macchine difficili o impossibili da potenziare, le cui componenti sono spesso proprietarie o sostituibili solo dalla casa produtrice, con un ciclo di vita mediamente più breve di un desktop. Una frase specifica del Manifesto rimane emblematica:
"In molti sostengono che i new media sono rivoluzionari e che la rete è anarchica e sovversiva. Ma come si può essere sovversivi in un club esclusivo, con una tassa d'ingresso di 1000 dollari? Lowtech è opposto a esclusività. Lowtech è la tecnlogia della strada."
Se già dal '99 trovare un vecchio Mac nella spazzatura è sempre più facile, FOSS (Free Open Source Software) e il riuso dell'hardware chiudono finalmente il cerchio: il Manifesto Lowtech è pronto.

DAL ONE LAPTOP PER CHILD DI NEGROPONTE ALLO ZDLT

Mentre al MIT Negroponte enuclea l'idea di One Laptop per Child, il famoso pc da 100$ per i bambini dei paesi in via di sviluppo, Wallbank continua la sua ricerca. A Sheffield, città in cui vive e lavora, nasce Access Space, spazio per le comunità locali dedicato all'inclusione digitale, al riuso, alle tecnologie libere. A otto anni di distanza, nel 2007, un nuovo Manifesto è divulgato: Zero Dollar Laptop. Tecnicamente ZDLT è un pc riciclato su cui viene installato software libero, pensato per paesi "sviluppati" e "in via di sviluppo", a uso di individui, organizzazioni non profit e business oriented, governi. I requisiti dell'hardware sono così descritti: 500 mHz, RAM da 256 mb, hard disk da 10 gigabyte, scheda di rete, CD-ROM, porta USB, schermo da 800x600 pixel a colori (16-bit). Concettualmente ZDLT è una piattaforma di educazione/produzione permanente e in continua evoluzione grazie al lavoro degli sviluppatori di free/open source software. Obiettivo: empowerment degli individui. Inoltre, tolti i costi organizzativi e di formazione (in sintesi, il lavoro dell'equipe), il laptop di Wallbank costa 0 dollari. Anche l'impatto ecologico è 0: questi laptop sono rifiuti riportati in vita.

Zero Dollar laptop: non solo qualche foto ricordo dei workshop ma sopratutto l'orgoglio di ridare vita a ipotetici rifiuti. Un'operazione "contro" la società dei consumi che vede l'IT tra i protagonisti indiscussi.

I BARBONI DI ST. MUNGO'S

Il laptop di Negroponte entra in produzione nel 2009: un'azione globalmente supportata da governi, media, centri di ricerca, istituzioni locali, ONG. Wallbank, in UK, lavora ai bordi del sistema: nello stesso anno Access Space inizia un dialogo con Furtherfield.org con l'obiettivo di creare i presupposti affinchè ZDLT si concretizzi in un progetto.

La fase di elaborazione dura circa un anno, durante il quale si definiscono l'identità e gli aspetti operativi dell'operazione: un programma di inclusione digitale che non esitiamo a definire radicale. I destinatari scelti saranno infatti gli homeless di St Mungo's, associazione di volontari che assicura assistenza, cibo e 100 posti letto ai barboni dell'area sud di Londra. Il programma consiste in una serie di workshop alla fine dei quali ogni partecipante entra in possesso del suo laptop, se ha assicurato una frequenza costante. Il programma parte a gennaio 2010 e dura due mesi, per un totale di 8 incontri settimanali. Il tutto si svolge nel quartier generale della St Mungo's: in tutto sono circa 20 gli homeless che aderiscono all'iniziativa, il doppio rispetto alle previsioni iniziali, tanto che alla terza settimana i promotori si vedono costretti a sdoppiare le lezioni fra mattina e pomeriggio. L'equipe, formata da Jake Harries and James Wallbank (Access Space), Ruth Catlow, Marc Garrett e Olga Panades (Furtherfield) parte dalle basi: installare una Linux Ubuntu distribution sulle macchine, studiare le componenti hardware, familiarizzarsi alla command line, imparare a usare Gymp, Open Office e a gestire il proprio indirizzo e-mail. Ma si va anche oltre, confrontandosi con lo spazio pubblico e facendo del proprio laptop un oggetto unico: ogni barbone gestisce un blog su wordpress e interagisce sui social network (incluso un gruppo Facebook dove condividere materiali e raccontare le proprie storie), mentre alcune lezioni sono interamente dedicate alla personalizzazione della macchina attraverso stencil, sfondi, immagini digitali. I laptop sono stati reperiti attraverso donazioni e infine acquisiti su eBay a 50$ l'uno per far fronte all'allargamento del gruppo. Questo elemento ci dà un indicazione precisa dell'impatto del progetto, in una comunità potenzialmente così difficile da approcciare. Mentre si attende il rinnovo dei fondi da parte dell'Art Council of London, ad oggi unico ente che ha supportato a livello finanziario l'iniziativa, i promotori, con Furtherfield in testa, si stanno organizzando per provare a mettere in piedi una rete europea di soggetti interessati a sperimentare e a replicare in altri luoghi ZDLT. Proprio in questo momento, alla Comunità Europea è in corso di valutazione un progetto presentato insieme ad altri tre paesi: Francia, Spagna e Italia (in partnership con Binario Etico). Abbiamo dunque qualche speranza di vedere ZDLT anche qui da noi.

RIFLESSIONI SULL'ACCESSO

Industria, stati, istituzioni – in sintesi il potere – decidono di supportare il laptop di Negroponte. Nel 2010, mentre i primi barboni di St Mungo's iniziano a smanettare sulle loro macchine riciclate, un modello nuovo fiammante di laptop entra in produzione per essere distribuito ai "bambini del terzo mondo".

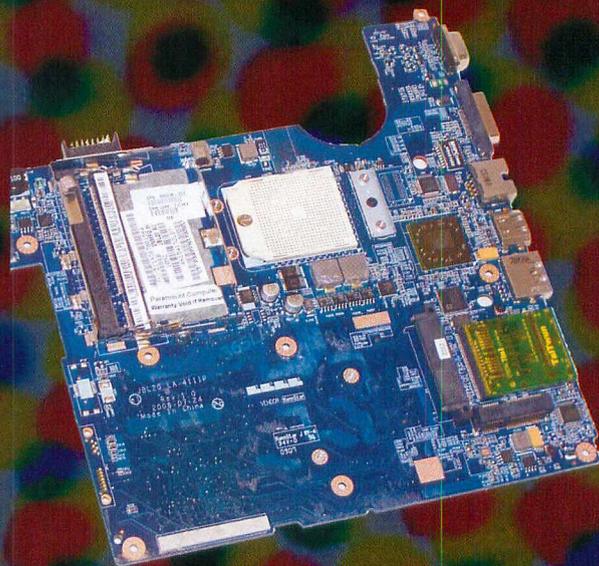
A favore di chi? Perchè? Con quale visione di accesso e inclusione? Vi lasciamo con qualche riga di Wallbank, che sul tema si è espresso in questi termini:

"È un processo ancora top-down, attraverso cui ricche e potenti istituzioni decidono "la soluzione" e la distribuiscono a quelle povere e più deboli, che a loro volta la distribuiscono a soggetti il cui ruolo è essenzialmente passivo".

Non solo uno slogan: tecnica, etica ed estetica insieme per una rivoluzione che parte dal modo di pensare all'IT.

di Little Rose
redazione@hackerjournal.it

IL RIUSO VINCENTE

UN COMPUTER ROTTO È LA SCUSA TROVATA PER UN HOME ENTERTAINEMENT VERAMENTE SPECIALE.

Avevo un bellissimo HP Pavilion comprato 3 anni fa ed ancora in ottimo stato e mi si sono rotti i supporti del monitor. Dopo un po' mi ha lasciato il masterizzatore DVD. Una disgrazia, certo, ma non come quella capitata a una mia amica a cui è saltata la scheda video integrata, fuori garanzia. Io mi sono arrangiata con dello scotch che ha tenuto il monitor per qualche tempo ma, poi, ho scoperto che il televisore della sala aveva l'ingresso PC ed è stato un chiodo fisso: volevo collegarci un computer che potesse farmi da centro multimediale. Certo, ho un lettore Blu Ray, ho il decoder per il satellite... Volete mettere con un computer con cui giocare (con monitor enorme), scaricare film e così via?
Così mi sono informata e la mia amica aveva un Pavilion un po' più recente del mio: aveva una faccia strana quando ho fatto un salto di gioia.

FATTO A PEZZI

Per prima cosa mi sono fatta dare il suo computer, ho svitato un po' di viti ed ho estratto il suo HDD. L'ho inserito nel mio portatile, che aveva spazio per un secondo hard disk, il tempo sufficiente per copiargli i dati su un HDD esterno. Poi ho fatto letteralmente a pezzi il resto del suo portatile perché volevo sperimentare lo smontaggio di un notebook. Non avevo mai avuto a che fare con i Pavilion e mi serviva una cavia. Così ho scoperto che ci sono pochissime viti che tengono il monitor mentre lo chassis principale richiede un po' di impegno: dopo aver aperto tutti gli sportelli raggiungibili e tolto le batterie mi sono ritrovata con una ventina di viti minuscole, scoprendo, tra l'altro, che una sola vite tiene in posizione il masterizzatore DVD. Masterizzatore: il mio era rotto ma quello non andava bene. La sua parte anteriore non combaciava con lo chassis. Ho fatto un po' di prove ed ho scoperto che bastava fare leva con un piccolo cacciavite per staccare il profilo esterno. Così ho fatto l'operazione anche sul mio, scoprendo che anche il suo profilo poteva staccarsi facilmente. Ho invertito i profili ed eccomi col masterizzatore nuovo (e il know-how per collegarlo al mio vecchio PC). Per quanto riguarda lo smontaggio, tolte le viti sul fondo, il resto è stato facile: un gioco di incastri e fili ben piegati che si innestavano sulla motherboard. Staccata la piattina, larghissima e sottilissima, che collegava il monitor, mi sono ritrovata con 5 cavi che uscivano dallo chassis principale: 2 per l'antenna Wi-Fi che aveva i terminali ai lati del monitor, uno di alimentazione del monitor, uno per la minuscola scheda che ospita la Webcam integrata e uno per i due microfoni (oppure un microfono stereo, che dir si voglia) che erano in alto al monitor. Passato l'attimo di vergogna perché non sapevo nemmeno di avere un microfono stereo, ho iniziato a staccare i cavi dalla motherboard, scoprendo che potevo rimuoverli tutti facilmente.

Tastiera wireless: costa 30 euro escluse spedizione e dogana. È in vendita su www.chinavasion.com.

WELCOME FRANKIE!

Il tavolo da lavoro sembrava l'incubo di qualsiasi elettronico ma mi sentivo sicura di riuscire a smontare la mia vecchia carriola per eliminare il monitor con lo scotch, i fili inutili e cambiare masterizzatore. Il secondo disco l'avevo già aggiunto. Così ho fatto un backup del mio disco (perché non si sa mai) ed ho iniziato a replicare quello che avevo fatto sul computer della mia amica. Ho rimosso con cura il monitor, ho aperto lo chassis sul lato inferiore e ho staccato i fili che avanzavano. Ho scoperto che, pur

essendo un modello più vecchio, il design interno era pressoché identico, con lievi differenze dovute al fatto che io avevo una tastiera più grande e più spazio per il secondo HDD. Alla fine delle operazioni, che hanno incluso lo smontaggio con chiave inglese dei supporti del monitor rotti, ho rimontato lo chassis, ho incrociato le dita e l'ho acceso: funzionava perfettamente. Alla fine ho ottenuto una specie di consolle degli anni '80 ma con la potenza di un moderno computer.

SOFTWARE E SO

Non potevo aspettare ed ho collegato un cavo monitor dall'uscita del computer al televisore. Windows Vista (usavo quello...) ha riconosciuto di non avere più il monitor principale ma che un altro monitor era collegato sull'uscita secondaria della scheda. Ammetto di essermi emozionata quando ho visto la schermata di loading di Vista sul televisore. Poi ho tolto la batteria (inutile e pericolosa se collegata in continuazione alla corrente elettrica) e ho collegato l'uscita cuffie del notebook all'ingresso line-in del televisore. Il lavoro, però, non era finito: dovevo decidere che SO usare perché di Vista ne avevo abbastanza. Così, trovandomi in casa una licenza Windows 7 Professional, ho deciso di usare quella. In realtà avrei potuto metterci un Linux ma, onestamente, non volevo qualcosa con cui lavorare: volevo una macchinetta da gioco. Così ho messo il CD di Windows 7 (purtroppo in inglese) e l'ho installato. Poi ho fatto quello che avrei fatto con qualsiasi altro computer: ho aggiornato il SO, ho aggiornato i driver hardware. Mi mancava la scheda Wi-Fi, staccata perché non avrei saputo dove collegare i cavi dell'antenna, ma ho avuto la fortuna di avere una presa LAN dietro alla TV e mi sono arrangiata con un cavo. Ho dovuto fare un po' di test con le impostazioni video perché Sony, che produce il mio televisore, non rilascia file .inf per Windows 7. Poco male: ho settato manualmente la scheda video per una risoluzione di 1080x768. Al sistema operativo di base, aggiornato, ho aggiunto Virtual CloneDrive, µTorrent e qualche altra utility carina.

Il mio televisore è un Sony Bravia con ingresso PC. Lo preferisco a quello HDMI: mi dà più controllo.

IL DIVERTIMENTO

Una volta ottenuto un sistema ben funzionante mi sono ricordata di aver letto su un vecchio HJ che si poteva collegare il WiiMote al PC. Ho sfogliato la collezione di riviste e l'articolo in questione mi ha acceso un'altra lampadina. Così sono uscita e mi sono comprata un WiiMote con una sensor bar non ufficiale (40 euro). Poi ho attaccato al mio nuovo-vecchio PC un dongle Bluetooth. L'articolo di HJ mi consigliava di usare lo stack Bluetooth prodotto dalla Blue Soleil (www.bluesoleil.com) e, dopo un po' di tentativi, me lo sono comprato online (meno di 20 dollari). Lo stack ha trovato subito il WiiMote e mi sono decisa a completare il collegamento usando GlovePie (glovepie.org/glovepie.php). Quest'ultimo programma è favoloso: puoi programmare il WiiMote per qualsiasi cosa ed è tutto scriptable. Così si può usare il WiiMote al posto del mouse. Il problema, però, restava la tastiera: se uno è sul divano, alzarsi per usare la tastiera non è comodo. Ho fatto un po' di ricerche, trovando una tastiera wireless grande poco più di un telecomando con tanto di touchpad per il controllo del cursore, online sul sito www.chinavasion.com. Alla fine, tra costo, spese di spedizione e tasse, l'ho pagata 60 euro e mi è arrivata in una settimana. Funziona benissimo e non ho dovuto configurare nulla: basta mettere il suo dongle in una porta USB e fa tutto da sola. Con tutto questo potevo giocare dal divano con il pad e la tastiera oppure caricare uno script di GlovePie e avviare uno qualsiasi

La scheda Wi-Fi interna agli HP Pavilion, in varie versioni. Inutilizzabile senza antenna. :-(

dei giochi che poi ho installato, ma mancava ancora qualcosa per far invidia agli amici. Così ho cercato tra i software che non usavo più, trovando Dragon Dictate Professional, e mi è venuta un'altra idea. Ho collegato un vecchio microfono alla mic-in del notebook ed ho installato il software Dragon. Dopo la canonica mezz'ora di addestramento, dal divano, ammetto che ora il mio sistema fa invidia anche a chi è decisamente più esperto di me perché, semplicemente, fa impressione: comando il sistema con la voce, gioco con grafica PC non avanzatissima ma ottima usando il WiiMote e navigo comodamente seduta con il mio tastierino. In più conto di recuperare almeno in parte i 150 euro spesi per i pezzi mancanti del sistema mettendo in vendita su eBay, come pezzi di ricambio, i monitor e le schede wireless recuperati da entrambi i notebook. Se non siete capaci di sistemarli voi, vengo io. Ormai sono pratica. ;-)

Il Wii Remote, oggetto del desiderio dei giocatori casalinghi. Con lo stack giusto è ideale anche per i giochi PC!

di G.Enoma
redazione@hackerjournal.it

IL PROGETTO "CAMPIONI DEL MONDO"

LE COMPETENZE CI SONO E ANCHE LA VOGLIA DI CONDIVIDERLE PER IL BENE DEGLI ALTRI. COME FARE A CONVERTIRE "BIT E NEURONI" IN "SORRISI"?

Questo articolo non è tecnico, ma essere Hacker non è solo un discorso di tecnica. Infatti è necessario mantenere un ruolo formativo integrale sulla figura Hacker e non solo passargli nozioni informatiche. Questo significa ricordargli obiettivi e valori.

SIAMO UOMINI O CAPORALI?

Senza offesa per i caporali, gente con i cosiddetti al posto giusto, la celeberrima frase di Totò stava a significare: "cosa ci distingue dagli altri"? Domanda attuale dato che certa stampa, pur di fare cassetta, non si preoccupa di distinguere le diverse sfaccettature di un mondo assai complesso e variegato. Capita quindi (con sommo dispiacere) di vedere etichettati come Hacker coloro che non sono altro che cracker, script-kiddies o lamer. Di fatto non si chiedono: cosa differenzia queste categorie di persone? Perché gli addetti ai lavori gli hanno assegnato nomi diversi? Eppure la differenza sarebbe facile da scoprire e facile da spiegare alle masse: basterebbe proprio chiedersi il "perché", la ragione che muove ciascuna di esse. Poi ci si accorgerebbe che come in tutte le cose non ci sono solo i buoni o solo i cattivi, e che entrambe queste figure convivono anche nel nostro mondo.

Sapere che ci sono "i buoni" anche nell'underground dell'hacking non va di moda e scompagina chi su tutto questo fraintendimento ci lucra pesantemente. Che succederebbe se si riuscisse ad associare agli Hacker comportamenti che ne dimostrino i valori, con benefici che esulano dal mondo prettamente IT?
Allora il cosiddetto "uomo quadratico medio" inizierebbe a porsi delle domande... e porsi delle domande è ciò che, sappiamo, fa migliorare le cose. In questo articolo vorrei suggerire (in punta di piedi) la strada che ho sperimentato personalmente, e che spero possa stimolare in voi quella voglia di essere Hacker fino in fondo.

ESSERE HACKER?

Dicesi "essere Hacker" (con la H maiuscola)... uhm... non è facile trovare una definizione. Sulle pagine di HJ abbiamo imparato che non significa alcune cose. Intanto che la conoscenza è un valore da coltivare, insieme allo spirito critico necessario per non dare nulla per scontato. Ma tutto ciò ancora non ci distingue dalle altre categorie del mondo dell'hacking. Infatti un valore altrettanto forte è quello della condivisione della conoscenza acquisita, senza secondi fini. Ovviamente ci vuole reciprocità, ma non si tratta di un "do-ut-des", cioè un "io ti dico questo solo se tu mi dici quello". Si tratta piuttosto di "ognuno mette in comunione le conoscenze che ha". Bene. Ci siamo finora distinti da lamer e script-kiddies: i primi non condividono nulla, mentre i secondi non capiscono le conoscenze che usano. Ma ancora c'è da differenziarsi.

Qui entra il punto più importante, quello che divide Hacker da cracker: il "perché" si agisce. I cracker infatti sono animati da due distinte motivazioni: il vantaggio personale a discapito di altri, o il desiderio di rivalsa contro altri. In altri termini: egoismo o vendetta. Il valore che l'Hacker porta avanti è quello del "insieme e per", opposto al "io e contro".

MA PARLA COME MANGI!

Li chiamavano *Spazzini*, poi sono diventati *Collaboratori Ecologici*. Li chiamavano *Orfanotrofi*, ora si dice *Case Famiglia*. La società moderna è diventata brava a giocare con i termini per addolcire le realtà più crude. L'obiettivo è positivo, ma il risultato è di rendere meno pressante l'interesse delle persone, che associano il nome più soft ad una realtà meno dura. Ed invece la realtà rimane dura e cruda. Ho conosciuto bene il mondo degli Orfanotrofi e mi è capitato più volte di pormi domande difficili. Ve ne passo una soltanto: "a che serve saper seguire un singolo bit nel suo flusso tra CPU, registri e stack, quando un bambino sta male di notte e non ha un papà a cui chiedere aiuto, o fa il compleanno e non ha una mamma con cui soffiare le candeline?" Mettetevi nei suoi panni. Una realtà dura e cruda. Per tanto tempo non ho trovato risposta, ma lo spirito Hacker non mollava la presa.

LA GESTIONE (ETICA) DEL TEMPO

Parliamo di tempo libero. Tutti ci lamentiamo di non averne, ma si può dimostrare con tecniche di Time Management che in realtà ciascuno di noi ne ha molto, che viene speso in modo spesso inconsapevole. C'è un problema oggettivo che ne rende difficile l'utilizzazione, specialmente se lo si vuole usare per fini non egoistici ("insieme e per"): molto di questo tempo è frammentato. Eppure tanti piccoli intervalli, se utilizzati bene, potrebbero fare molto!

Luogo di realizzazione	Attività	Minori inseriti	Status del progetto
MYANMAR (ex Birmania) *diverse localita' del Myanmar*	garantire un'opportuna istruzione, oltre ad un contributo per le necessita' di base quali alimentazione, vestiario, cure mediche, per favorire, in un domani, un adeguato accesso al mondo del lavoro.	344	in espansione
MYANMAR (ex Birmania) *diverse localita' del Myanmar*	garantire un'opportuna istruzione, oltre ad un contributo per le necessita' di base quali alimentazione, vestiario, cure mediche, per favorire, in un domani, un adeguato accesso al mondo del lavoro.	283	in espansione
FILIPPINE *Quartiere di San Isidor (Davao)*	Scuola materna, alimentazione, vestiario, prevenzione e cure sanitarie, sostegno alle famiglie	192	in espansione
FILIPPINE *La Union (250 Km nord di Manila)*	Pre-scuola, alimentazione, vestiario, prevenzione e cure sanitarie; accompagnamento e corsi per genitori.	227	in espansione
FILIPPINE *Quartieri di Tramo e Tambo*	12 diversi programmi di sviluppo per l'infanzia (istruzione materna, elementare, alimentazione, interventi sanitari, attivita' ricreative). Sostegno alle famiglie, counselling, microcredito per miglioramento abitativo. E' stato realizzato un centro sociale con aule, ambulatori, laboratori.	746	in espansione
FILIPPINE *Quartiere di Mabolo - (citta' di Cebu)*	Prescuola, dopo-scuola, alimentazione, prevenzione sanitaria. Corsi per genitori (alfabetizzazione, sartoria, igiene). Realizzato un Centro Sociale con aule, ambulatori, ambienti per attivita' comunitarie	302	in espansione

Un esempio delle opportunità di SAD (Sostegno a Distanza) offerta da una delle associazioni autorizzate.

IL PROGETTO CAMPIONI DEL MONDO

Sarebbe bello se si svuotassero gli orfanotrofi e tutti avessero una famiglia. Sappiamo che per svuotare qualcosa bisogna prelevarne il contenuto, impedendone al contempo gli ingressi. I processi di adozione nazionale e internazionale operano per svuotarli, ma bisogna anche evitare che continuino a riempirsi. Sopratutto nei paesi in via di sviluppo, la causa prima è l'indigenza delle famiglie di origine. E a ciò si può porre rimedio, come fanno le iniziative di SAD (Sostegno a Distanza): aiutare la famiglia di origine in modo che egli possa rimanere con loro, creando occasioni di lavoro per i genitori e curando aspetti sanitari e formativi del bambino. Ricapitolando, l'equazione era: come posso tradurre quel tempo libero così sfuggente e quelle conoscenze acquisite con fatica, in un modo per aiutare bambini ad avere una famiglia? Ho trovato che trasformare la conoscenza in articoli e/o libri permette di trasformare parti di tempo libero (anche le più piccole) in un qualcosa che poi a sua volta può essere usato per sostenere un bambino tramite un SAD. Siccome tra il dire e il fare..., nel 2008 creai il progetto "Campioni del Mondo". L'obiettivo visibile era sostenere parallelamente 11 bambini, a rappresentanza dei 4 angoli della terra, in modo che potessero crescere e rendersi autosufficienti rimanendo nelle loro famiglie. Ma si propone anche di dimostrare con i fatti che ciascuno di noi, con un po' di organizzazione e buona volontà, ma sopratutto con un desiderio vero di condivisione "insieme e per" può tradurre "bit e neuroni" in "sorrisi". Ad oggi il progetto conta già 4 SAD concorrenti attivi, e cresce in modo progressivo e sostenibile, senza intaccare né il tempo dedicato alla altre cose di prima, *né il bilancio familiare*.

DA QUI IN POI

Se in tanti seguissero l'idea e creassero un loro progetto "Campioni del Mondo" potremmo veramente fare la differenza per molti bambini. Si potrebbe creare una rete per dare visibilità del risultato complessivo (pur nel sacrosanto diritto alla privacy dei beneficiari). Ma chi potrebbe voler aderire? Chi ha conoscenze di qualità ed è ben disposto a condividerle in modo altruistico? Ad ognuno la propria risposta. Personalmente ho notato che la voglia di apprendere ha ora una marcia in più. Il contributo di ciascuno di noi al problema è come una piccola goccia, ma anche un oceano è fatto di gocce. E noi siamo tanti...

PER APPROFONDIRE

Qualche link alle informazioni utilizzate nella stesura dell'articolo:

- www.edc-consulting.org – Il sito che contiene, anche, il progetto Campioni del Mondo
- www.time-management.it – Tecniche di Time Management